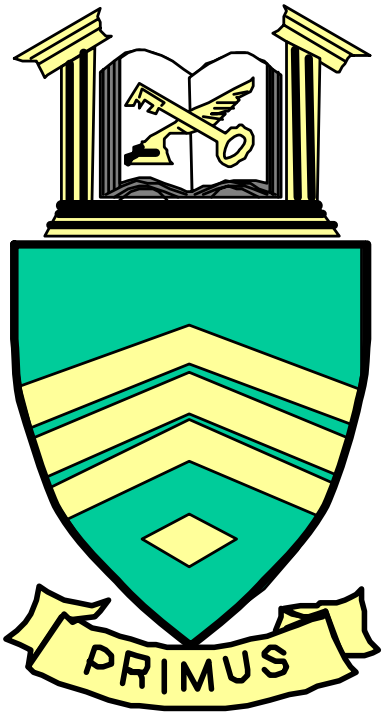
U.S. ARMY SERGEANTS MAJOR ACADEMY (FSC-TATS)

R652 (052002) JUN 01

PHYSICAL SECURITY

# PRERESIDENT TRAINING SUPPORT PACKAGE



# Overview

Part of your responsibility as a senior unit leader is to assist the commander in safeguarding all supplies and equipment within the unit. You must have an understanding of the installation commander's responsibilities as well as your unit commander's responsibilities. The reading assignments in this lesson will reinforce your knowledge of the requirements relating to physical security and help you perform your duties in this area. This lesson consists of five (5) Student Handouts, a Lesson Exercise, and a Solution/Discussion for the Lesson Exercise.

# Inventory of Lesson Materials

Prior to starting this lesson ensure you received all materials required for this Training Support Package. Go to the "**This [TSP or Appendix] Contains**" section, on page two of the TSP and the first page of each Appendix, and verify you have all the pages. If you are missing any material, contact the First Sergeant Course Class Coordinator at the training institution where you will attend phase II FSC-TATS.

# Point of Contact

If you have any questions regarding this lesson, contact the First Sergeant Course Class Coordinator at the training institution where you will attend phase II FSC-TATS.

| | |
|---|---|
| **TSP Number/ Title** | R652, Physical Security |
| **Effective Date** | JUN 01 |
| **Supersedes TSPs** | R652, Physical Security, NOV 99 |
| **TSP User** | This TSP contains a training requirement that you must complete prior to attending phase II, FSC-TATS. It will take you approximately 3 hours to complete this lesson. |
| **Proponent** | The proponent for this document is the U.S. Army Sergeants Major Academy. POC: FSC TATS Course Chief, DSN: 978-8854/8848; commercial: (915) 568-8854/8848 |
| **Comments and Recommen-dations** | Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to:<br><br>ATTN ATSS DCF FSC<br>COMDT USASMA<br>BLDG 11291 BIGGS FLD<br>FORT BLISS TX 79918-8002 |
| **Foreign Disclosure Restrictions** | The lesson developer in coordination with the USASMA foreign disclosure authority has reviewed this lesson. This lesson is releasable to foreign military students from all requesting foreign countries without restrictions. |

**This TSP Contains**

The following table lists the material included in this TSP:



## SECTION I ADMINISTRATIVE DATA

**Tasks Trained**

This lesson trains the tasks listed in the following table:

| | |
|---|---|
| **Task Number:** | 191-000-0003 |
| **Task Title:** | Develop a unit physical security plan, |
| **Conditions:** | as a first sergeant, given AR 190-11, AR 190-51, AR 380-5, |
| **Standards:** | IAW AR 190-11, AR 190-51, and AR 380-5. |

**Task Reinforced**

None

**Prerequisite Lessons**

None

**Clearance and Access**

There is no clearance or access requirement for this lesson.

**Copyright Information**

No copyrighted material reproduced for use in this lesson.

**References**

The following table lists the reference(s) for this lesson:

| Number | Title | Date | Additional Information |
|---|---|---|---|
| AR 190-11 | Physical Security of Arms, Ammunition and Explosives. | Feb 98 | |
| AR 190-51 | Security of Unclassified Army Property (Sensitive/Non-sensitive). | Sep 93 | |
| AR 380-5 | Department of the Army Information Security Program. | Sep 00 | |

**Equipment Required**

None

**Materials Required**

None

**Safety Requirements**

None

**Risk Assessment Level**

Low

**Environmental Considerations**

None

**Lesson Approval** The following individuals reviewed and approved this lesson for publication and incorporation into the First Sergeants Course-The Army Training System.

| Name/Signature | Rank | Title | Date Signed |
|---|---|---|---|
| Kevin L. Graham | MSG | Training Developer | |
| Chris L. Adams | SGM | Chief Instructor, FSC | |
| John W. Mayo | SGM | Course Chief, FSC-TATS | |

## SECTION II INTRODUCTION

**Terminal Learning Objective** At the completion of this lesson, you will

| | |
|---|---|
| **Action:** | Identify the policies and procedures for unit physical security, |
| **Conditions:** | as a first sergeant in a classroom environment, given an extract of AR 190-11 (SH-1), an extract of AR 190-51(SH-2), and an extract of AR 380-5 (SH-3), |
| **Standard:** | Identified the policies and procedures for unit physical security IAW SH-1, 2, and 3. |

**Evaluation** Before entering Phase II FSC-TATS, you will receive an end of Phase I exam that will contain a 50-question written objective examination. It will test your learning of the objectives from this and other lessons. To get a go (70 percent), you must answer 35 or more of the questions correctly.

**Instructional Lead-in** Knowing, and practicing, proper physical security procedures within your unit will keep you, your commander, and your unit, from undergoing costly and time consuming problems.

## SECTION III PRESENTATION

**ELO 1**

| | |
|---|---|
| **Action:** | Determine security requirements for Army property at unit level, |
| **Condition:** | as a first sergeant in a classroom environment, given SH-2, |
| **Standard:** | Determined security requirements for Army Property at unit level IAW SH-2. |

**Learning Step/Activity (LS/A), 1 ELO 1**

To complete this learning step activity, you are to

- Read the above ELO.
- Study Student Handout 2, extract of AR 190-51.
- Complete Items 1, 2, and 3, of the Lesson Exercise at Appendix B, without referring to the student handouts.
- Compare your responses with the suggested solution found in SLE-1 solution/discussion for lesson exercise 1 (Appendix B).
- If your response does not agree, review the appropriate reference/lesson material.

**ELO 2**

| | |
|---|---|
| **Action:** | Identify the basic policy and security requirements for safeguarding, storing, and handling arms, ammunition, and explosives, |
| **Condition:** | as a first sergeant in a classroom environment , given SH-1, |
| **Standard:** | Identified the basic policy and security requirements for safeguarding, storing, and handling arms, ammunition, and explosives IAW SH-1. |

**LS/A 1, ELO 2** To complete this learning step activity, you are to

- Read the above ELO.
- Study Student Handout 1, extract of AR 190-11.
- Complete Items 4, 5, and 6, of the Lesson Exercise at Appendix B, without referring to the student handouts.
- Compare your responses with the suggested solution found in SLE-1 solution/discussion for lesson exercise 1 (Appendix B).
- If your response does not agree, review the appropriate reference/lesson material.

**ELO 3**

| | |
|---|---|
| **Action:** | Identify the four security risk categories of AA&E, |
| **Condition:** | as a first sergeant in a classroom environment, given SH-1, |
| **Standard:** | Identified the four security risk categories of AA&E IAW SH-1. |

**LS/A 1, ELO 3** To complete this learning step activity, you are to

- Read the above ELO.
- Study Student Handout 1, extract of AR 190-11.
- Complete Items 7 and 8 of the Lesson Exercise at Appendix B, without referring to the student handouts.
- Compare your responses with the suggested solution found in SLE-1 solution/discussion for lesson exercise 1 (Appendix B).
- If your response does not agree, review the appropriate reference/lesson material.

**ELO 4**

| | |
|---|---|
| **Action:** | Identify the special requirements for storing arms, |
| **Condition:** | as a first sergeant in a classroom environment, given SH-1, |
| **Standard:** | Identified the special requirements for storing arms IAW SH-1. |

**LS/A 1, ELO 4** To complete this learning step activity, you are to

- Read the above ELO.
- Study Student Handout 1, extract of AR 190-11.
- Complete Item 9 of the Lesson Exercise at Appendix B, without referring to the student handouts.
- Compare your responses with the suggested solution found in SLE-1 solution/discussion for lesson exercise 1 (Appendix B).
- If your response does not agree, review the appropriate reference/lesson material.

**ELO 5**

| | |
|---|---|
| **Action:** | Identify the requirements to protect privately owned weapons on installations or facilities, |
| **Condition:** | as a first sergeant in a classroom environment, given SH-1, |
| **Standard:** | Identified the requirements to protect privately owned weapons on installations or facilities IAW SH-1. |

**LS/A 1, ELO 5** To complete this learning step activity, you are to

- Read the above ELO.
- Study Student Handout 1, extract of AR 190-11.
- Complete Item 10 of the Lesson Exercise at Appendix B, without referring to the student handouts.
- Compare your responses with the suggested solution found in SLE-1 solution/discussion for lesson exercise 1 (Appendix B).
- If your response does not agree, review the appropriate reference/lesson material.

**ELO 6**

| | |
|---|---|
| **Action:** | Identify the uses of Standard Forms 700, 701, and 702, |
| **Condition:** | as a first sergeant in a classroom environment, given SH-3, |
| **Standard:** | Identified the uses of Standard Forms 700, 701, and 702 IAW SH-3. |

**LS/A 1, ELO 6** To complete this learning step activity, you are to

- Read the above ELO.
- Study Student Handout 3, extract of AR 380-5.
- Complete Item 11 of the Lesson Exercise at Appendix B, without referring to the student handouts.
- Compare your responses with the suggested solution found in SLE-1 solution/discussion for lesson exercise 1 (Appendix B).
- If your response does not agree, review the appropriate reference/lesson material.

## SECTION IV SUMMARY

**Review/ Summarize Lesson**

This completes the lesson on physical security. The knowledge you gain from this lesson will give you the opportunity to enhance the physical security program at your unit while you assist your commander in this very important area. Remember, the S-2 and Provost Marshal are resources you can also call on to ensure that you are taking the proper physical security actions to protect your unit to assist in accomplishment of the mission.

**Check on Learning**

The Lesson Exercise in Appendix B serves as the Check on Learning for this lesson.

## SECTION V STUDENT EVALUATION

**Testing Requirements**

Before entering phase II FSC-TATS, you will receive the end of phase I Performance Examination that will include questions based on material contained in this lesson. On that examination, you must answer 35 or more, out of 50 questions, correctly to achieve a GO. A GO is a requirement for graduation.

## SECTION VI STUDENT QUESTIONNAIRE

**Directions** Complete the following blocks:

- Enter your name, your rank, and the date you complete this questionnaire.

| Name: | Rank: | Date: |
|---|---|---|
| | | |

- Answer items 1 through 6 below in the space provided.
- Fold the questionnaire so the address for USASMA is visible.
- Print your return address, add postage, and mail.

Note: Your response to this questionnaire will assist the Academy in refining and improving the course. When completing the questionnaire, answer each question frankly. Your assistance helps build and maintain the best Academy curriculum possible.

| | |
|---|---|
| **Item 1** | Do you feel you have met the learning objectives of this lesson? |
| **Item 2** | Was the material covered in this lesson new to you? |
| **Item 3** | Which parts of this lesson were most helpful to you in the learning objectives? |
| **Item 4** | How could we improve the format of this lesson? |
| **Item 5** | How could we improve the content of this lesson? |
| **Item 6** | Do you have additional questions or comments? If you do, please list them here. You may add additional pages if necessary |

Place
1st Class
Stamp
Here

ATTN ATSS DCF FSC TATS
COMDT USASMA
BLDG 11291 BIGGS FLD
FT BLISS TX 79918-8002

# Appendix B

## Index of Lesson Exercises and Solutions

**This Appendix Contains**

This Appendix contains the items listed in this table--

# Lesson Exercise 1

| | |
|---|---|
| **Title** | Determine Appropriate Physical Security Doctrine |
| **Introduction** | As a first sergeant, you need to know how to determine appropriate physical security doctrine. |
| **Motivator** | This practical exercise will give you experience in applying proper physical security measures using appropriate doctrine. |
| **Safety Requirements** | None |
| **Risk Assessment Level** | Low |
| **Environmental Considerations** | None |
| **Evaluation** | This is not a graded exercise. You have a solution to this lesson exercise which you should review upon completion of the eleven items. |
| **Instructional Lead-in** | None |
| **Resource Requirements** | None |
| **Special Instructions** | • You should be able to answer the 11 multiple choice questions within 25 minutes.<br>• Be sure to time yourself when you start and select only one answer for each question. |

**Item 1** Which of the following is a minimum physical protective measure for night vision devices in the unit?

A. Light the storage area during the hours of darkness.

B. Provide double barrier protection.

C. Secure in a class 5 vault or comparable container.

**Item 2** How often must you check keys to locks in use which protect property in an office, unit, or activity?

A. Annually.

B. Semiannually.

C. Quarterly.

D. At the end of each duty day.

**Item 3** What is the minimum requirement to inventory padlocks and their keys?

A. Weekly

B. Monthly

C. Quarterly

D. Semiannually

**Item 4** The unit commander's responsibilities for arms, ammunition, and explosives (AA&E) security include compliance with AR 190-11, reporting all losses to law enforcement agencies, and _____.

A. conducting checks, inventories, and inspections of AA&E storage facilities.

B. selecting AA&E storage sites, and controlling AA&E issue.

C. training AA&E control officer.

**Item 5** Security requirements for AA&E during training include continuous positive control of AA&E, no unattended or unsecured AA&E, and _____.

A. a roving patrol

B. deadly force briefing to everyone involved in the training

C. an armed guard

D. an available response force to protect AA&E

**Item 6** Training requirements for personnel responsible for the security and accountability of AA&E include care and use of weapons, guard orders, and _____.

A. common forms of sabotage and espionage

B. knowledge of local MP areas of responsibility

C. perimeter establishment for exclusion area

**Item 7** How many security risk categories of military arms (including missiles and rockets) does the Army have?

A. Two

B. Three

C. Four

**Item 8** How many security risk categories of ammunition and explosive does the Army have?

A. Three

B. Four

C. Five

**Item 9** When does a storage structure containing Category II arms require the use of armed guards?

A. After duty hours, weekends, and holidays.

B. Constantly, unless the intrusion detection system is operational.

C. When the commander orders constant surveillance.

**Item 10** The requirements to protect privately owned weapons on installations include briefing all new personnel, securing items in unit arms room or other authorized locations, and _____.

A. cleaning of privately owned weapons monthly.

B. coordinating safety inspections of privately owned weapons by the provost marshal.

C. requiring personnel with privately owned weapons and ammunition to attend weapons safety classes.

D. requiring the commander or his authorized representative to approve withdrawal of privately owned AA&E from the unit arms room.

**Item 11** What form would you use to perform the end-of-day check of your security container?

A. Department of the Army Form 3964.

B. Standard Form 701a.

C. Standard Form 702.

D. Standard Form 1222.

# Solution to Lesson Exercise 1

**Title** Determine Appropriate Physical Security Doctrine

**Item 1** Which of the following is a minimum physical protective measure for night vision devices in the unit?

B. Provide double barrier protection.

Ref: SH-2-7, AR 190-51, para 3-6b(1) (ELO 1)

**Item 2** How often must you check keys to locks in use which protect property in an office, unit, or activity?

D. At the end of each duty day.

Ref: SH-2-9, AR 190-51, App D, para D-6a (ELO 1)

**Item 3** What is the minimum requirement to inventory padlocks and their keys?

D. Semiannually.

Ref: SH-2-9, AR 190-51, App D, para D-6b (ELO 1)

**Item 4** The unit commander's responsibilities for arms, ammunition, and explosives (AA&E) security include compliance with AR 190-11, reporting all losses to law enforcement agencies, and _____.

C. Conducting checks, inventories, and inspections of AA&E storage facilities.

Ref: SH-1-4, AR 190-11, para 1-10i (ELO 2)

**Item 5** Security requirements for AA&E during training include continuous positive control of AA&E, no unattended or unsecured AA&E, and ___.

D. an available response force to protect AA&E.

Ref: SH-1-7, AR 190-11, para 2-5d (ELO 2)

**Item 6** Training requirements for personnel responsible for the security and accountability of AA&E include care and use of weapons, guard orders, and ____.

D. common forms of sabotage and espionage.

Ref: SH-1-10, AR 190-11para 2-10b(8) (ELO 2)

**Item 7** How many security risk categories of military arms (including missiles and rockets) does the Army have?

C. Four.

Ref: SH-1-25, AR 190-11, App B, para B-2a and b (ELO 3)

**Item 8** How many security risk categories of ammunition and explosive does the Army have?

E. Four.

Ref: SH-1-26, AR 190-11, App B, para B-2c (ELO 3)

**Item 9** When does a storage structure containing Category II arms require armed guards?

B. Constantly, unless the intrusion detection system is operational.

Ref: SH-1-20, AR 190-11, para 4-2f(1) (ELO 4)

**Item 10** The requirements to protect privately owned weapons on installations include briefing all new personnel, securing items in unit arms room or other authorized locations, and ____.

D. requiring the commander or his authorized representative to approve withdrawal of privately owned AA&E from the unit arms room.

Ref: SH-1-24, AR 190-11, para 4-5b(4) (ELO 5)

**Item 11** What Standard Form would you use to perform a daily check of your security container?

C. Standard Form 702, Security Container Checksheet.

Ref: SH-3-3, AR 380-5, para 6-10 (ELO 6)

# Appendix C

## Index of Student Handouts

**This Appendix Contains**

This Appendix contains the items listed in this table:

# Student Handout 1

This handout contains extracts of AR 190-11 and AR 190-13 you will need to study to complete this lesson.

***(Start of extract of AR 190-11)***

Army Regulation 190-11

Military Police

**Physical Security of Arms, Ammunition, and Explosives**

12 February 1998

Effective: 12 March 1998

Unclassified

1-1. Purpose

*a.* This regulation prescribes standards and criteria for the physical security of sensitive conventional arms, ammunition, and explosives (AA&E), including nonnuclear missiles and rockets, as set forth in appendix B, in the custody of any Department of the Army (DA) Component, or contractor and subcontractor. (See app H for AA&E physical security standards at contractor facilities.) This regulation also prescribes policy, procedures, and standards, and assigns responsibilities for the effective implementation and application of physical security of AA&E.

*b.* Although the standards and criteria in this regulation will provide adequate protection against loss or theft or AA&E at most DA activities, and Department of Defense (DOD) (DA) contractor activities, the threat or characteristics of a particular location may require increased measures subject to approval by the major Army commands (MACOMs) concerned. MACOMs will establish procedures to review the justification of military construction projects that exceed the criteria in this regulation. This regulation does not authorize methods or operations inconsistent with AR 385-64, paragraphs 1 through 12 and appendix A.

*c.* The provisions of this regulation apply to sensitive conventional arms, ammunition and explosives as follows:

(1) *Arms*. Weapons that will, or are designed to, expel a projectile or flame by the action of an explosive and the frame or receiver of such weapons and comparable foreign arms, U.S. prototype arms and illegally manufactured arms which are retained in the inventory for training, familiarization, and evaluation. This includes handguns, shoulder-fired weapons, light automatic weapons up to and including .50 caliber machine-guns, multi-barrel machine-guns such as the 7.62mm M134, recoilless rifles up to and including 106mm, mortars up to and including 81mm, man-portable rocket launchers, flame-throwers, and individually operated weapons that are portable or can be fired without special mounts or firing devices and that have potential use in civil disturbances and are vulnerable to theft. Comparable foreign arms, U.S. prototype arms, and illegally manufactured weapons retained in the inventory for training, familiarization, and evaluation are also included.

(2) *Ammunition*. A device charged with explosives, propellants, pyrotechnics, initiating composition, riot control agents, chemical herbicides, smoke and flame for use in connection with defense or offense including demolition and having, in general, an individual or unit of issue, container, or package weight of 100 pounds or less. Included are rounds of 40mm and larger; conventional, guided missile, and rocket ammunition weighing 100 pounds or less per round; and 1,000 or more rounds of ammunition smaller than 40mm; and, other ammunition specified in appendix B. Ammunition excluded from the specified requirements of this regulation are the following:

(*a*) Devices charged with nuclear or biological agents;

(*b*) Devices charged with chemical agents, except for those specified in appendix B;

(*c*) Blank ammunition, .22 caliber rimfire ammunition, inert training ammunition;

(*d*) Artillery, tank, mortar ammunition 90mm and large, and naval gun ammunition 3 inches, 76mm, and larger. However, this ammunition requires Transportation Protective Service as set forth in chapter 7.

(3) *Explosives*. Any chemical compound, mixture, or device, the primary purpose of which is to function by explosion. The term includes, but is not limited to, individual land mines, demolition charges, blocks of explosives and other explosives consisting of 10 pounds or more. The scope of this regulation additionally includes and is limited to:

(*a*) Categorized explosives specified in app B.

(*b*) Uncategorized Class A and B explosives when being transported (see chap 7).

*d.* AA&E items covered by this regulation that are also classified will be stored and transported per AR 380-5, appendix H, AR 55-355, chapter 34, and this regulation. Where specific individual requirements differ between these regulations, the more stringent requirement will be followed.

*e.* MACOMs will prescribe physical security requirements for AA&E items outside the scope of this regulation. Consistent with operational and safety requirements and this regulation, physical security requirements for production and manufacturing operations at Government facilities

will be prescribed by the Joint Ordnance Commanders' Group (JOCG).

*f.* The criteria in this regulation are intended for sites where AA&E are maintained on a permanent basis during daily peacetime conditions, and not for training, contingency sites or operations, such as wartime, force generations, exercises, or operational readiness inspections. For sites and operations not specifically covered in this regulation, MACOMs will establish requirements and procedures to provide protection for AA&E consistent with the philosophy of this regulation, when operationally and environmentally feasible. Upon declaration of war, commanders may prescribe procedures suspending specific physical security provisions of this regulation to account for local conditions, while ensuring maximum practical security for Government personnel and property. This authority is granted to installation, division, and separate brigade commanders and may be delegated to commanders in the grade of lieutenant colonel. Upon mobilization (prior to a declaration of war), this authority is granted to commander of MACOMs and may not be further delegated. In the above circumstances (declaration of war or mobilization), suspension of transportation physical security requirements will be coordinated promptly with HQDA (DAMO-ODL and DALO-TSP) and with the Commander (CDR), Military Traffic Management Command (MTMC).

g. The Army's inventory of AA&E is a vital part of its readiness posture. Loss or theft of such material can foster fear in the public sector and create an image of the Army's inability to secure its assets. The degree of security to provide AA&E is contingent upon many variables. It is impractical, therefore, to pre-scribe definitive DA physical security standards to cover all anticipated conditions that could impose a threat to the security of the items to be protected. Minimum physical security standards are prescribed in this regulation. As the criminal or other type threats to these materials increase at the local level, security measures at that level may need to be more stringent than those prescribed in this regulation. Commander will notify Headquarters, Department of the Army (HQDA) immediately through commander channels local resources are inadequate to provide necessary protection.

### 1-5. HQDA staff agencies, MACOMs, Army National Guard of the United States, and installation commanders

Heads of HQDA staff agencies, MACOMs, Army National Guard of the United States, and installation commanders will support the AA&E physical security program according to prescribed responsibilities in AR 190-13, paragraph 1-5 and this regulation.

*a.* All commanders will apply enough human resources and funds to A&E physical security programs at all levels.

*b.* MACOM commanders will identify resource needs in the planning, programming and budgeting system, and allocate necessary resources to support their AA&E physical security program. Installation commanders will ensure funds identified for physical security are used as intended.

### 1-10. Commanders and custodians of AA&E

Commanders and custodians of AA&E will--

*a.* Comply with this regulation.

*b.* Ensure necessary measures are taken to safeguard AA&E at all times. This includes providing specific instructions on individual responsibility for AA&E during operational or field training conditions, care and maintenance, competitive marksmanship meet, and storage on, or when mounted on, vehicles and aircraft.

*c.* Ensure timely submission of serious incident reports (SIR) per AR 190-40, paragraph 4-9.

*d.* Report all losses (actual or suspected) or recoveries within 2 hours of initial detection to the proper law enforcement agencies.

*e.* Conduct prompt investigation of losses after a decision of the USACIDC that criminal acts were not involved.

*f.* Fix responsibility when negligence is determined and take proper corrective action to prevent further loss.

*g.* Publicize AA&E security and loss prevention through command information and unit training programs.

*h.* Plan, program, budget, and allocate resources for the implementation of required policies outlined in this regulation.

*i.* Ensure that AA&E storage facilities are checked, inventoried, and inspected as required by this regulation.

1-11. Active Army installation commanders, Reserve Component commanders, and unit commanders

Active Army installation commanders, Reserve Component (RC) commanders, and ROTC unit commanders will--

*a.* Coordinate physical security plans with local LEAs and supporting military intelligence (MI) and USACIDC elements.

*b.* Set up liaison at the local level with the agencies per chapter 3.

*c.* Ensure that agreements governing consolidated AA&E storage facilities and the storage of AA&E property of Federal, State, contractor agencies, and foreign government agencies contain definite assignment in writing of responsibility for the items stored.

*d* Conduct unannounced inspections as often as deemed necessary by the commander concerned.

*e.* Ensure construction programming documents involving AA&E facilities have been coordinated with the responsible provost marshal or security officer.

1-12. Commanders or directors of activities, installation planning boards, and responsible or accountable officers

*a.* Commanders or directors of activities, and units on Active Army installations, or subinstallations, will coordinate physical security plans for standard operating procedures (SOPs) once a year with the installation PMO or Security Office. They will--

(1) Ensure their security procedures are current and in keeping with the command and HQDA physical security directives.

(2) Include provisions in security procedures for applying physical security measures for storage areas in keeping with the host commanders assessment.

*b.* Commanders or directors of tenant activities (located both on and off the installation) must identify their security requirements to the host installation. They will ensure funding provisions are considered in proper budget programs.

*c.* Installation planning boards will include a physical security representative from the LEA, PMO or Security Office as a voting member on all actions. The representatives will ensure that provisions of this regulation are considered and made a matter of record during the planning process.

*d.* This regulation does not relieve responsible or accountable officers of this responsibility to account for property.

*e.* Persons issued or holding AA&E are responsible for properly securing such property while it is charged or entrusted to their care.

1-13. Security of nonsensitive AA&E

AA&E that does not meet the criteria in this regulation for "sensitive" items must be safeguarded from pilferage, theft, and wrongful destruction when stored or deployed in the field. Although this regulation does not prescribe security criteria for these items, AR 190-13, para 1-5, assigns commanders the responsibility to ensure reasonable security measures are taken to safeguard property and facilities that may be vulnerable to criminal acts or other disruptive activities. Commanders and security personnel involvement is necessary to ensure that the security measures taken provide enough security based on an assessment of the threat and vulnerability of the items concerned. Such security measures can include use of fences, lighting, locks and key control, security patrols, and any other measures deemed suitable by the commander responsible for the security of the items involved.

Chapter 2, Policy

2-1. General

*a.* Systems should incorporate technology and equipment available within the Federal Government and the private sector to provide cost effective protection, automated accountability, and inventory control. Physical security equipment management policy is established in AR 190-13, chapter 4. Security criteria will be included in initial plans for research and development, as well as all new or modified construction projects.

*b.* To minimize the cost of physical security and inventory control, and to reduce theft vulnerability, the quantities of AA&E and the number of storage facilities for AA&E should be reduced. Storage should be consolidated to the maximum extent

consistent with operational, safety, and training requirements.

(1) AA&E should be removed from designated storage areas as briefly as possible. The quantity to be removed should be as small as possible to support specific missions or projects. Storage areas should be as small as possible consistent with safety standards, security, and mission requirements.

(2) Further reduction of costs for protection and inventory control can be effected by grouping the consolidation of AA&E into smaller storage areas by assigned risk category, and providing the degree of physical security protection needed for that category. Priority attention will be given to demilitarization or disposal of obsolete and unserviceable AA&E to avoid unnecessary storage, security, and inventory-related costs.

(3) The provisions of this regulation are intended to provide adequate storage security for AA&E at most DA activities. There may be a few unusual activities, such as large depots or remote storage areas without existing electrical service, where not all criteria in this regulation can be directly applied in a cost effective manner. At these unusual or unique facilities, local conditions must be carefully evaluated, and the security system must be tailored to the local conditions, based on practicability and cost, rather than specific security requirements prescribed herein. In these instances, waivers or exceptions should conform to the requirements provided in paragraph 2-4.

2-2. Construction of facilities

*a.* The provisions of this regulation are mandatory for new construction of permanent land-based installations for storage of sensitive AA&E. Modification to existing facilities will be accomplished in accordance with the criteria set forth in this regulation.

*b.* The tearing down and rebuilding of facilities will not be undertaken unless the concerned MACOM has determined that existing security measures cannot be supplemented to provide the required degree of protection. When nonstandard structures or facilities provide equivalent or better protection, modifications will not be undertaken. Exceptions to this policy will be granted under paragraph 2-4.

*c.* Upgrading of existing storage structures must be consistent with approved plans for future development and new construction plans. The type, planned use, modification costs, and remaining economic life of storage structures must be considered. Additionally, in determining upgrade requirements, ammunition and explosives will be consolidated by risk category to the maximum extent consistent with operational, safety, and training requirements. Compensatory security measures will be established for AA&E storage structures that do not meet minimum construction standards. Definitive drawings and specifications for new construction, upgrade, or modification of AA&E storage structures will be coordinated with the engineer office, safety office, and LEA, PMO, or security police office to ensure safety and physical security requirements are met.

*d.* Qualified engineer personnel will verify the structure composition of AA&E storage facilities (for example, walls, ceilings, roofs, floors, and doors). Statements will be prepared on DA Form 4604-R (Security Construction Statement). Statements will indicate the highest construction category met for storage of AA&E, for example, Category I, II, III, or IV AA&E items and date of applicable regulation. (See para 2-4 for procedures when structural deficiencies exist.) The DA Form 4604-R will be affixed to the interior wall of each AA&E storage facility. The DA Form 4604-R will be locally reproduced on 8½-x 11-inch paper. A copy for reproduction purposes is located at the back of this publication. A blanket statement on DA Form 4604-R may be issued at an installation for all facilities, such as ammunition magazines, constructed according to the same specifications. Under these circumstances a copy of the DA Form 4604-R need not be affixed to the interior wall of each individual storage structure, but must specifically identify the facilities by number and location, and be readily available for inspection. Security construction statements will be reviewed during physical security surveys and inspections. The statements will be revalidated by engineer personnel every 5 years.

*e.* Physical security personnel will monitor construction of new facilities and renovation of existing facilities. Engineer personnel will coordinate new construction and renovation projects with the local

provost marshal or security officer. In addition to meeting construction standards, storage of AA&E will meet physical security criteria, such as Intrusion Detection System (IDS), locks and hasps, lighting, and security patrols, as necessary, for the particular category of AA&E involved.

### 2-3. Priority lists

The MACOMs will establish a priority list for meeting the security requirements. Requirements will be listed in priority sequence by category for planning, programming, and budgeting purposes. Priority of installation of IDS is as follows:

*a.* Facilities storing Category I items, when protection is inadequate. Those having the largest quantity will receive initial attention.

*b.* Facilities storing Category II items.

*c.* Facilities storing Category III items.

*d.* Facilities storing Category IV items.

*e.* Deviations from these priorities will be permitted only when MACOMs have determined that a local threat dictates these deviations.

### 2-4. Waivers and exceptions

Commanders are authorized 10 percent deviation from the physical security construction standards established by this regulation for existing facilities. Otherwise waivers and exceptions to the physical security requirements of this regulation must be granted by the DCSOPS or his or her delegated authority in accordance with the procedures established by HQDA (DAMO-ODL) under the following provisions:

*a.* Waiver and exceptions will be considered individually: blanket waivers and exceptions will not be authorized. Requests for waivers or exceptions applying to commercial carrier's transportation minimum security standards (chap 7), together with compensatory measures taken, will be forwarded through the Commander, Military Traffic Management Command, ATTN: MT-SS, 5611 Columbia Pike, Falls Church, VA 22041, to HQDA (DAMO-ODL-S), 400 ARMY PENTAGON, WASH DC 20310-0400.

*b.* Waivers normally may be granted for a period of 1 year and may be extended only after a review of the circumstances necessitating the extension. Waivers will not exceed 2 years when resource considerations clearly indicate a continued waiver requirement beyond the normal 1 year waiver period. Justification for such waivers will be required. Each extension will state first extension, second extension, and so forth.

*c.* Exceptions will be granted only when correction of a deficiency is not feasible or when the security afforded is equivalent to or better than that afforded under the standard criteria.

*d.* Requests for waivers and exceptions will contain compensatory measures in effect or recommended. Approvals for waivers and exceptions will specify required compensatory measures. Equivalent protection exceptions do not require compensatory measures.

*e.* Deficiencies that will be corrected within 60 days will not require a waiver or exception; however, compensatory measures will be taken during the interval.

*f.* Authority to grant waivers and exceptions constituting standards below those prescribed in this regulation must be approved by the DCSOPS or his or her designated authority. U.S. Army Reserve Command requests for waivers and exceptions will be submitted through command channels through the Commander, U.S. Forces Command, Fort McPherson, Georgia 30330-6000, to HQDA (DAMO-ODL-S), 400 ARMY PENTAGON, WASH DC 20310-0400.

*g.* Requests for physical security waivers or exceptions will be coordinated between the LEA, PMO, or security office of the installation or activity. When structural deficiencies exist, requests also will be coordinated with the supporting engineer.

*h.* A request for a physical security waiver or an exception will include--

(1) A statement of the problems or deficiencies that constitute standards below those cited in this regulation.

(2) Compensatory measures in effect at AA&E storage facilities to make up for noncompliance with required standards of protection.

(3) Reasons the unit, facility, or installation cannot comply with the requirements of this regulation.

(4) The commander's statement of corrective action taken or planned to correct the deficiencies for which the waiver or exception is required.

(5) Each successive command's recommendation.

*i.* The unit and the approving headquarters will retain on file the approved waiver or exception, including the documents listed in *c* above.

*j.* Exceptions will be regarded as generally permanent; however, they will be reviewed at least once every 2 years to determine if they need to be continued. The review will be conducted by the authority who approved the exception.

*k.* Exceptions previously granted under the criteria of the previous AR 190-11 remain valid under the provisions of this regulation. Such exceptions need not be resubmitted for approval. However, such exceptions will be reviewed as indicated in paragraph *j* above.

### 2-5 Security of AA&E during training, and aboard ships

Specific criteria and standards for protection of AA&E during training and in shipboard armories or otherwise on board ships will be developed by the MACOM concerned, based on the security philosophy in this regulation. AA&E deployed in the field for training or operational purposes will be secured at all times. The deploying commander will establish and enforce procedures for securing deployed AA&E based on an assessment of the threat, objectives, location, and duration of the deployment. The following guidelines apply:

*a.* AA&E will be under continuous positive control.

*b.* AA&E will not be left unattended or unsecured.

*c.* Persons charged with custody of AA&E will have the capability to sound the alarm if a forceful theft is attempted.

*d.* A response force will be available to protect the AA&E.

*e.* A system of supervisory checks will be established to ensure all personnel comply with security procedures. Supervisory checks of the AA&E holding area will be made to ensure the AA&E being guarded have not been tampered with.

*f.* Control of ammunition and explosives during field training or range firing will be monitored closely by all officers, noncommissioned officers (NCOs), or civilian equivalents. Upon completion of training, the area(s) will be policed and unused ammunition and explosives collected for turn-in. Personnel will be checked closely to ensure unused ammunition and explosives are not retained. Close supervision by officers, NCOs, or civilian equivalents can eliminate most security problems in the training area.

*g.* Selection of personnel to perform guard duties at AA&E holding areas will be closely monitored by commanders to ensure only responsible individuals are assigned duty.

### 2-6. Inspections and audits

Security measures including theft or loss reporting and inventory and accountability procedures for AA&E will be examined during inspections and audits. The status of existing waivers and exceptions will be examined for compliance and continuing necessity.

*a.* Physical security inspections will be conducted according to AR 190-13, paragraphs 2-11, on facilities in which AA&E governed by this regulation are stored. Additionally, conduct physical security surveys and inspections as follows:

(1) For new AA&E storage facilities, before and immediately after occupancy.

(2) On significant change in facility structure.

(3) After a forced entry or attempted forced entry with or without theft.

(4) When units have received an unsatisfactory rating on physical security survey/inspection, reinspection will be within 6 months. A copy of an unsatisfactory physical security survey or inspection concerning RC and ROTC units will be furnished the installation commander providing logistical report. The follow-up report will include written comments to show what elements have received copies.

*b.* Physical security inspections of AA&E deployed in the field for training and operations will be conducted to ensure these items are properly protected.

*c.* Results of physical security inspections and surveys will be briefed to the commander responsible for the security of the facility or area inspected.

*d.* Inventory, accountability, issue and turn-in procedures will be included in physical security inspections/surveys to ensure the procedures support the physical security program. AR 710-2, chapter 2, applies to supply operations below the

wholesale level. AR 740-26, chapter 2, establishes physical inventory controls at the wholesale level. Chapter 4, this regulation, applies regarding accountability requirements for contractor owned and commercial arms and ammunition.

*e.* When custody of arms storage facilities is transferred between authorized persons, they will conduct a physical count of the weapons and ammunition stored therein, per requirements in AR 710-2, paragraphs 2-12 and 2-53; and DA Pam 710-2-1, paragraph 9-11. The inventory and change of custody will be conducted and recorded per AR 710-2, paragraphs 2-12 and 2-53; and DA Pam 710-2-1, paragraph 9-11.

### 2-7. Prohibition

*a.* Gun clubs and activities under the responsibility of the Director of Marksmanship are not authorized to possess or store Category I or Category II AA&E. The Army National Guard and reserves are not permitted permanently to store Category I AA&E. However, with prior HQDA (DAMO-ODL) approval, they are authorized to temporarily store (not to exceed 90 days) Category I AA&E at ammunition supply points for training of Army National Guard and reserve units. Additionally, Army National Guard and reserve units are authorized temporary custody (not to exceed 14 days) of Category I AA&E for training on military installations. In both instances, physical security measures in chapter 5 and paragraph 7-15*c* of this regulation must be followed.

*b.* Reserve Officers Training Corps (ROTC/ JROTC) units are not authorized to possess or store Category I AA&E. ROTC units (with the exception of Norwich University, Virginia Military Institute, Texas A&M, the Citadel, and North Georgia College) and gun clubs are not authorized to permanently possess or store Category II AA&. ROTC units may retain temporary (overnight/weekend) custody of AA&E for training purposes. This temporary custody will not exceed 72 hours. Physical security measures in chapter 4 will be adhered to.

*c.* ROTC units may use Category II weapons for familiarization training and field training exercises or marksmanship, on or off a military reservation. Active Army installations, RC facilities and National Guard units are encouraged to provide support to ROTC units when requested.

### 2-8. Requisition

HQDA (DALO-SMP-S) will establish procedures for item managers to ensure necessary requisition verification of AA&E items. Commanders will include instructions to ensure AA&E requisitions are authorized by designated personnel and released only to properly identified authorized personnel. The procedures will include positive steps for rejecting excess and unauthorized requisitions. (See AR 710-2, para 2-52, for policy on requisitioning.)

### 2-9. Investigations

A thorough investigation will be made of lost, stolen, or missing AA&E to determine the circumstances surrounding the loss or theft and to fix responsibility as necessary. Inventory and accountability losses will be investigated thoroughly. Before any loss can be attributed to any inventory or accountability discrepancy, it must be determined through investigation that the loss was not the result of theft or misappropriation, per AR 735-5, chapter 13, as appropriate.

*a. Guidance on actions to be taken*. Active Army and RC commanders, or their designated representatives, having direct responsibility for AA&E lost, stolen or missing or the receiving unit or agency will--

(1) Notify the supporting LEA, PM, or security office as soon as the incident is discovered. The notice will be as complete as possible but will not be delayed because of incomplete data. USAR will notify the PMO or LEA responsible for the geographical area. In CONUS, this notice will include the proper FBI field office having area jurisdiction. Civil authorities in overseas areas will be notified according to local policy.

(2) When sensitive AA&E are reported lost, a preliminary investigation will be conducted by the USACIDC to determine criminality before beginning any administrative action (see para 1-4).

(3) Start administrative action per AR 735-5, chapter 13, if the USACIDC investigation determines a crime was not committed. The report of survey or an equal procedures will not be used as a disciplinary or punitive measure. The use of this administrative procedure will not prevent recourse

to disciplinary measures when proper. Therefore, the survey will not be used instead of a criminal investigation when one is warranted.

(4) Determine accountability for recovered property per AR 735-5, paragraphs 14-16 and 14-17. A person may be held responsible and be required to pay for a loss. If so, he or she will not be allowed to claim title or obtain ownership of the item if it is recovered.

(5) Consider relative investigative findings in violation of this or other applicable regulations. Take proper punitive action if events warrant.

(6) Request, through channels, that an AR 15-6 investigation be initiated for AA&E in appendix E. This may be used instead of a Report of Survey per AR 735-5, paragraph 13-2.

*b. Property overages*. Property overages will be handled in the same way as stated in *a* above.

*c. The investigation*. Facts must be presented by the requesting person. The installation, depot, or community commander may then direct that an investigation by initiated. The officer appointed to conduct the investigation will follow procedures per AR 15-6, chapters 3, 4, and 5, and this regulation.

*d. In-transit losses*. Consignees of AA&E shipments will report in-transit losses to the supporting LEA, PMO, or security office.

*e. Inventory adjustments*. Inventory losses or overages may be determined as administrative, computer, or other type accountability errors and not actual losses. This determination will be made only after investigative action has established the cause of the discrepancy. (In no case may a weapon, ammunition, or explosive loss or overage be attributed to inventory error unless the responsible agency, unit, or activity conducts an investigation that, beyond a doubt, excludes the possibility of theft or loss.) When such a decision has been made, DA Form 3056 (Report of Missing/Recovered Firearms, Ammunition and Explosives) will be submitted (fig 2-1). The form will explain--

(1) The rationale for such a decision.

(2) The type of inventory adjustment action taken.

(3) The name, grade, and duty position of the approval authority.

*f. Transportation losses*. Transportation officers, or their designated representatives, will inform the supporting LEA, PMO, or security office when claims or other data reflect the loss of AA&E from shipment or storage. This report will include household goods and losses of privately-owned weapons.

*g. Competitive marksmanship weapons.* Members of the Civilian Marksmanship Program will report the loss of AA&E to the local police or Federal Bureau of Investigation (FBI), and the director of the program.

*h.* Criminal investigation reports. The CG, USACIDC will provide HQDA (DAMO-ODL-S), upon request, copies of completed criminal investigation reports. The reports will describe the loss or theft of AA&E. Reports prepared by the FBI will be included as attachments or as received.

### 2-10. Training

*a.* Commanders responsible for AA&E will establish a training program for those personnel responsible for the accountability of these items. The training program will be designed to--

(1) Provide training in inventory and accountability procedures as outlined in applicable 700-series Army regulations.

(2) Fit the requirements of different groups of personnel responsible for accountability.

(3) Indoctrinate personnel in the principles, criteria, and procedures for accountability and inventory, including disciplinary actions against individuals responsible for violating security requirements as prescribed in this regulation.

*b.* Commanders will initiate an aggressive training program to ensure all unit personnel are aware of their responsibilities for the security and accountability of AA&E. A training program will also be established to ensure requirements of AR 190-56, chapter 4, are kept and to ensure continued proficiency of the guard force. As a minimum, this training will include--

(1) Care and use of weapons, to include qualification firing with assigned weapons within the past 12 months.

(2) Legal authority, responsibility, and jurisdiction of guards on duty, to include apprehension, search and seizure, and use of force.

(3) Physical fitness training.

(4) Guard orders, to include communications and duress procedures.

(5) Duties in the event of emergencies, such as alerts, fire, explosion, civil disturbance, intrusion, attempted seizure, or terrorist incident.

(6) Current criminal threat to AA&E.
(7) Crime prevention.
(8) Common forms of sabotage and espionage, to include current threat situation.
(9) Location of hazardous and vulnerable equipment and materiel, to include high security risk AA&E requiring special attention or more frequent security checks.
(10) Location of fire protection equipment, decontamination stations, electrical switches, and first aid facilities.
(11) Operation and monitoring of intrusion detection system.
(12) Additional training subjects are listed in AR 190-13, paragraph 2-5.

*c.* Commanders will take continuing action through annual update refresher briefings to ensure that all personnel are aware of their responsibilities for the control and safeguarding of AA&E.

2-11. Personnel

*a.* Commanders will be selective in assigning personnel to duties involving control of AA&E. Only personnel who are mature, stable, and have shown a willingness and capability to perform assigned tasks in a dependable manner will be assigned to duties which involve responsibility for the control, accountability, and shipment of AA&E. As part of this selection process, personnel assigned duties involved in the control, accountability, and shipment of AA&E will be screened and evaluated using DA Form 7281-R (Command Oriented Arms, Ammunition, and Explosives (AA&E) Security Screening and Evaluation Records). DA Form 7281-R may be locally reproduced on 8½- x 11-inch paper. A copy of this form for reproduction purposes is located in the back of this handbook. Completed forms will be retained on file within the command until the individual departs, or is relieved of his or her AA&E oriented duties. In addition, MACOMs will implement procedures to ensure the following:

(1) Any Government employee (civilian or military) or DA contractor (including commercial carrier) employee operating a vehicle or providing security to a vehicle transporting Category I, II, or classified AA&E will as a minimum have been the subject of a favorable National Agency Check (NAC) or Entrance National Agency Check (ENTNAC), per AR 380-67, paragraph 3-613, except as provided below.
(2) Officers of U.S. flag carriers will be licensed in accordance with U.S. Coast Guard requirements.
(3) Designated carrier employees providing Protection Security Service for the transportation of items classified SECRET will possess a Government-issued SECRET clearance per AR 380-67, paragraph 3-613, and carrier issued identification.
(4) In situations or at locations where these requirements cannot reasonably be accomplished, a properly cleared escort will be provided to accompany the shipment and prevent unauthorized access. Procedures that address these concerns will be prepared by the cognizant security office and will include statements regarding two-person rule and other specific procedures, as appropriate.

*b.* Commanders will determine the reliability and trustworthiness of the following personnel before they are assigned duties involving control of AA&E:
(1) Personnel authorized unaccompanied access to arms, and Category I and II ammunition and explosives storage facilities.
(2) Personnel authorized to receive, store, or issue arms and Category I and II ammunition and explosives at such storage facilities.
(3) Personnel authorized to issue or control keys to AA&E storage facilities in (1) and (2) above.

*c.* Commanders will prohibit access to above personnel when doubt exists as to their reliability or trustworthiness. All personnel will be required to undergo a command oriented security screening or an equivalent foreign country check before access is authorized. The security screening check will be designed to provide the commander reasonable assurance that personnel with character traits that raise significant doubt as to their honesty or stability are not afforded access. At a minimum, the command oriented security screening will include:
(1) A personal interview of the individual conducted by his or her immediate commander or supervisor.
(2) A request for medical file check of active duty military personnel.
(3) A personnel records check.
(4) A records check of the provost marshal or security office.

(5) A records check of local civilian law enforcement agencies in the area of the person's residence if permitted by state or local laws.

*d.* Commanders may deny access to the above personnel when doubt exists as to their reliability or trustworthiness. The following disqualifying factors will be considered:

(1) Record of alcohol abuse.

(2) Record of unauthorized use, sale, or possession of drugs and narcotics.

(3) Record of mental instability or disorders.

(4) Record of judicial or nonjudicial punishment.

(5) Pattern of behavior or actions which are reasonably indicative of a contemptuous attitude toward the law.

(6) Any other character trait, or a record of conduct, or adverse information, which, in the commander's judgment, would be prejudicial to reliability or trustworthiness.

*e.* Continuing evaluation of all personnel is essential to the success of the AA&E security screening policy. All personnel involved in AA&E will be fully cognizant of their responsibilities to observe and report promptly to the commander any incident or condition which might result in temporary or permanent disqualification of such personnel. Security screening checks in *c* above will be repeated every 3 years.

## Chapter3, Physical Security Planning

### 3-1. General

In assessing local requirements for protection, the following factors should be considered:

*a.* Threat assessment based on information furnished by local intelligence, criminal investigative, or law enforcement agencies.

*b.* Types of AA&E, other sensitive assets, property maintained and mission of the facility.

*c.* Location, size, and vulnerability of storage facilities.

*d.* Vulnerability of AA&E to theft and loss.

*e.* Geographic location within the installation and relative to surrounding population centers.

*f.* Availability and responsiveness of security forces.

*g.* Availability or existence of security enhancing systems, including:

(1) Perimeter barriers.

(2) Security lighting.

(3) Communication systems.

(4) Key and lock controls.

(5) Stringent construction criteria for storage areas and armories.

(6) Personnel and vehicular entry control.

(7) Security training programs.

(8) IDS (including closed circuit television (CCTV).

(9) Military Working Dogs.

(10) Security guard personnel.

### 3-2. Coordination

*a.* In developing a security plan, coordination and close liaison should be effected between the military commander and--

(1) Adjacent installations or units.

(2) Federal agencies.

(3) State and local agencies.

(4) Similar host country agencies.

*b.* To the extent permissible, such interaction should allow for an exchange of intelligence information on security measures being employed, contingence plans, and any other information to enhance local security.

*c.* On an installation, the host activity will assume responsibility for coordinating physical security efforts of all tenants, regardless of the DOD components represented, as outlined in the support agreements and the host activity security plan. Applicable provisions will be included in, or be an appendix to, the support agreement.

(1) Bilateral storage agreements will be used when--

(a) AA&E are stored on the installations or facilities of other U.S. or foreign government agencies or other DOD services.

(b) Consolidated storage facilities are used to store AA&E belonging to more than one unit or organization.

(2) A formal agreement will contain definite assignment of physical security responsibility for the items stored. The agreement will address--

(a) Maximum quantities to be stored.

(b) Physical safeguards to be used.

(c) Frequency of and the responsibility for physical inventories or reconciliation's.

(d) Reporting of losses for investigations.

(e) Key control procedures.

(f) Unit that has overall responsibility for the storage facility.

(g) Procedures for authorization and identification of individuals to receipt for physically taking custody of AA&E.

(h) Risk Categories of items to be stored.

*d.* The formal agreement concerning physical security requirements for AA&E can be implemented by an appendix to a host/tenant activity support agreement or by a Letter of Instruction (LOI).

*e.* The purpose of such coordination is protection in depth. Authority, jurisdiction, and responsibility must be set forth in a manner that ensures protection and avoids duplication of effort.

### 3-3. Contingency plans

In most instances it will be necessary to increase security for AA&E and other sensitive property, assets and facilities during periods of natural disasters, natural emergencies, or periods of increased threat from terrorist or criminal elements. Therefore, contingence plans should include provisions for increasing the physical security measures and procedures for storage areas based on the local commander's assessment of the situation. These provisions should be designed for early detection of an attempted intrusion, theft, or interruption of normal security conditions.

### 3-4. Security threats

*a.* The security plan will provide for the identification of local threats and should make full use of the investigative resources available in the geographic area to anticipate criminal activities that threaten the physical security of AA&E assets. At a minimum, liaison shall be established with the following agencies.

(1) Local Federal Bureau of Investigation field office.

(2) Local law enforcement agencies.

(3) Intelligence and investigative agencies of the Uniformed Services.

(4) Bureau of Alcohol, Tobacco, and Firearms field office.

(5) Host country agencies where applicable.

*b.* Installation plans shall address actions to counter thefts by employees. These actions include personnel screening (see para 2-12) and the monitoring to minimize opportunities for employee theft and to detect concealed shortages.

*c.* The USACIDC is designated as the single MACOM for receiving, analyzing, and disseminating data on the criminal threat to the security of the United States Army. The U.S. Army Intelligence and Security Command (INSCOM) will perform a similar function as related to terrorist, hostile intelligence, demonstrator, and hostile special operation threats.

*d.* Commanders responsible for storage of AA&E will--

(1) Coordinate with local USACIDC and Military Intelligence (MI) elements to receive current data on any threat to the security of these items. USACIDC and MI personnel shall conduct periodic visits with commanders or their designated representatives. These visits should provide updated threat analysis data based on observed vulnerabilities.

(2) Assess the local requirements for physical security protection.

(3) Incorporate into local security plans or SOPs, procedures for providing the following essential elements of criminal data to the nearest MP and USACIDC representatives as the data become available.

(a) Any intent to steal AA&E.

(b) Suspicious acts indicating that a storage area is being targeted by criminal elements.

(c) Alleged offers to buy or barter for AA&E.

(d) Losses of AA&E, including alleged inventory or administrative errors, together with the events surrounding individual losses.

### 3-5. Implementation of physical security planning

Commanders at each installation, unit or activity will--

*a.* Issue instructions regarding all phases of security operations pertinent to the installation, unit or activity. These instructions will be reviewed at least annually for relevance and currency.

*b.* Develop and implement an effective security awareness program based on current physical security plans.

*c.* Develop effective countermeasures to prevent or reduce the risk posed by potential threats.

(1) Countermeasures should be consistent with the current physical security plan and the requirements of Army physical security regulations and MACOM supplements.

(2) Physical security countermeasures consist of measures and procedures designed to reduce risk by--

(a) Providing means of alerting response forces to the presence of intruders as soon as possible.

(b) Providing means of delaying intruders long enough to prevent intruders from completing the purpose of the intrusion.

(3) Physical security measures and procedures are specified in Army regulations and MACOM supplements and include--

(a) Area patrols.
(b) Continuous surveillance.
(c) Security fences, doors, walls and locks.
(d) Security vaults.
(e) Security lighting.
(f) IDS.
(g) CCTV.
(h) Clear zones.
(i) Response forces.

*d.* Sensitive or critical items or equipment should be stored in inner zones of an installation. This may require inventory, segregation, and restorage, where practical by risk categories.

*e.* Security protection requirements for AA&E will be based on the highest category item stored in magazines or other structures.

### 3-6. Intrusion Detection Systems

The IDS is an essential part of the physical security system. IDS consists of the combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into an area protected by the system. IDS includes both interior and exterior systems. The system will report directly to an alarm monitoring station. The system will be an approved DOD standardized system or a MACOM approved commercial system.

*a.* IDS will include a central control station where alarms will sound and from which a response force can be dispatched. An alarm bell located only at the protected location is not acceptable. The IDS will be designed to cause an alarm to sound at the central control panel whenever the system is turned off or malfunctions. Some means of communication will be provided between the protected areas and the monitoring area to coordinate status changes. Telephone communication should be considered. On and off, access, and secure switches not located at a central control station will be located within the alarmed area. The response force should respond to an activated alarm as soon as possible, but in no case may arrival at the scene exceed 15 minutes. Facilities off military installations, will have a local alarm in addition to monitoring capability. Alarm circuitry that requires alarm signals to be cleared either by the central control station alarm monitor or by entering the protected area will be used. Use of alarm delay switches at RC facilities is discouraged. AA&E storage facilities (other than bulk storage facilities) that require IDS will be protected by at least two types of sensors, one of which is a volumetric sensor. Additional levels of protection, when practical, are encouraged (e.g., duress signaling components) and will be considered for Category I and II arms storage facilities.

*b.* Facilities having IDS will have signs prominently displayed announcing the presence of IDS. They will be affixed at eye level, when possible, on the exterior of each interior wall that contains an entrance to the protected area. They will be affixed on exterior walls only when the exterior wall contains an entrance to the protected area. Specifications for IDS signs are per appendix F.

*c.* IDS will include a protected, independent, backup power supply that will provide a minimum of 4 hours of uninterrupted power, or other duration as outlined in the site survey.

*d.* Where an IDS is used in civilian communities, arrangements will be made to connect alarms to civil police headquarters, private security companies, or a monitoring service from which immediate response can be directed in case of unauthorized entry.

(1) A commercial answering service is not authorized.

(2) Coordination is required with civil authorities to ensure a response force can be directed to respond immediately.

*e.* A daily log will be maintained of all alarms received, and at a minimum will include--

(1) The nature of the alarm; for example, intrusion system failure or nuisance alarm.

(2) The date and time the alarm was received.

(3) The location, and action taken in response to the alarm.

*f.* Logs will be maintained for a minimum of 90 days and will be reviewed periodically to identify, monitor, and correct IDS reliability problems.

(1) DA Form 4930-R (Alarm/Intrusion Detection Record), may be used to record alarms received. DA Form 4930-R will be locally reproduced on 8½- x 11-inch paper. A copy for reproduction purposes is located at the back of this handbook.

(2) Computer generated printout of alarms may be used as a substitute provided all required information has been included or supplemental information is included in a log.

(3) Serious or recurring problem areas will be described in writing and sent through command channels to CDR, U.S. Army Belvoir R&D Center, ATTN: AMCPM-PSE, Fort Belvoir, VA 22060-5606.

*g.* Transmission lines for the alarm circuits will have line supervision (connecting lines will be electrically supervised to detect evidence of tampering or malfunction and any visible lines must be inspected weekly) or two independent means of alarm signal transmission from the alarm area to the monitoring station must be provided. One of the two independent means of alarm signal transmission must be either a long-range radio or cellular telephone link. Two undedicated, hardwire telephone links are not acceptable. The dual transmission equipment must continuously monitor the integrity of both the telephone wire line and cellular or long range radio links. Upon loss of either communication path, the system must immediately initiate notification to the monitoring facility via the other communication link. Because of the criticality of the information to be transmitted, the dual transmission equipment must be able to seize control of the communication links, even if that link is already in use. Physical protection of both communication links is critical. Therefore, the hardware communication links is critical. Therefore, the hardware communications link will be enclosed in metallic conduit from the protected area to wherever the communication is made to the telephone network. Communications equipment, including cellular equipment, will be mounted in tamper protected enclosures. Communications equipment, including cellular antennas where possible, will be located within the protected area. Additionally, a protected backup independent power source of 8 hours minimum duration will be provided. Telephone communication between a central control station and alarm zones to provide for controlled entry by authorized personnel should be considered as an adjunct to the IDS. Systems will be tested quarterly and a log maintained at least 1 year for recording all tests. Visible lines will be inspected on a regular basis.

*h.* Following requirements also apply:

(1) IDS will be considered for security classification if it meets the specific classifying criteria per AR 380-5, chapter 2 and appendix G. If classified, appropriate personnel security clearance must be obtained.

(2) Only authorized personnel should be allowed access to unclassified IDS installation wiring diagrams for a specific facility or location. This also applies to information on known, specific vulnerabilities or counter-measures affecting the IDS.

(3) Civilian employees whose duties involve the design, operation, or maintenance of IDS require completion of a favorable National Agency Check with written inquiries (NACI) prior to appointment to such noncritical-sensitive positions. Civilian contractor employees must possess a minimum security clearance of CONFIDENTIAL, granted in accordance with AR 380-67, paragraph 3-400.

(4) A check of the National Crime Information Center (NCIC) for installers and maintainers of unclassified IDS is a command decision. The decision will be based on--

(a) The sensitivity of the area to be protected.

(b) The need for quality control over personnel having access.

(5) All installers, maintainers, and operators of unclassified IDS will undergo a command-oriented security check. The security check should be made with the area provost marshal (PM) or other agencies that might have information on file bearing on the honesty or stability of the individual. Requirement for above command-oriented security checks should be based on local jurisdiction policies, the local threat and sensitivity, and vulnerability of the facility protected.

(6) All keys associated with IDS components will be safeguarded and controlled according to paragraph 3-8.

(a) Monthly Joint-Service Interior Detection System (J-SIIDS) operational checks to ensure

activation of the sensors will be conducted utilizing appendix K. In addition, a visual inspection of components and conduit for evidence of tampering will be conducted during the monthly inspection. Commercial intrusion detection systems employing sensors equipped with a remote-test feature that activate the same sensing phenomenology as would an actual intruder do not require operational checks by unit personnel. Each zone component will be checked and tested by alarm maintenance personnel a minimum of every six months during preventive maintenance. Commercial intrusion detection systems that do not have a remote-test feature will be tested monthly utilizing the manufacturers operational test.

(b) Installation physical security inspectors will include a check of each IDS during any security inspection to verify the IDS is operating satisfactorily. Checks will include inspection of components and conduit for evidence of tampering. Checks will also be made of unit log entries and records regarding operation and inspection of IDS.

(7) Before accepting a newly installed IDS system for operation, an inspection will be conducted by qualified technical personnel to ensure the system meets all minimum acceptable standards. The statement of verification will be maintained in the using unit or organization files. DA Form 4604-R may be used to record the verification.

(8) Maintenance of IDS will be provided by personnel qualified in installation and repair of IDS. Such maintenance will be performed consistent with operational requirements to ensure continuous operation and reliability of each system in use.

(9) All intrusion detection equipment enclosures with removable covers will be equipped with tamper switches. The tamper detection will be continuously monitored whether the system is in the "secure" or the "access" mode of operation. Enclosures that are not routinely opened for maintenance purposes (such as pull boxes) shall be equipped with tamper switches.

### 3-7. Security forces

A security or guard patrol or unit personnel will periodically check facilities and areas used to store sensitive or critical items or equipment as prescribed herein and as dictated by a threat and vulnerability analysis. Checks will be conducted on an irregular basis during nonduty hours to avoid establishment of a pattern. Security checks will be made to ensure unauthorized personnel are not in the area and the structures are intact and have not been broken into. During periods of increased vigilance because of a threat situation, security patrols will physically inspect doors and locks on all storage structures in their area of responsibility. Selection of personnel to perform guard duties will be closely monitored by commanders to ensure only properly trained and reliable individuals are assigned duty. Supervisory checks will be conducted to ensure guard duties are being performed properly.

*a.* Security patrols may be conducted by military personnel; civilian security personnel, including contract personnel; U.S. Marshal Service; or State, local, or campus police.

*b.* DA-controlled security forces will be provided with adequate means of communication.

*c.* Security forces personnel (e.g., guards, security patrols, security reaction forces) may be armed with appropriate weapons and ammunition at the discretion of the commander concerned. If such personnel are armed, provisions of AR 190-14, chapters 2 and 4 apply.

*d.* Guard procedures will be reviewed at least annually and revised if necessary to provide greater application of security measures, and will place special emphasis on guard post locations and guard orientation concerning duties to be performed.

*e.* Inspections and guard checks will be increased during nights, weekends, and holidays to provide for deterrence of violations and early detection of loss. These checks will be recorded and will consist of an inspection of the building or facility including all doors and windows. Records of these checks will be maintained in an active file for a minimum of 90 days, and then destroyed.

*f.* Law enforcement patrol plans will be coordinated and integrated with the guard plan or other security plans and programs to the maximum extent possible. When facilities are located in civilian communities, liaison will be established with local civil police agencies to ensure that periodic surveillance is conducted and that a coordination plan for security exits.

3-8. Key and lock controls

*a.* Only approved locks and locking devices (including hasps and chains) will be used. See the consolidated glossary for a list of DA-approved locks and hasps. All questions regarding the identity of approved commercial equivalent locks and locking devices (including hasps and chains) meeting Military Specifications will be addressed to the Naval Civil Engineering Laboratory (NCEL), Port Hueneme, CA. Personnel can obtain the most current version of the specifications by contacting the NCEL at DSN 360-5927 or (805) 982-5927. Keys will be signed out to authorized personnel, as needed, on a key control register. The DA Form 5513-R (Key Control Register and Inventory) is approved for use to meet the requirements of this regulation. DA Form 5513-R will be locally or electronically reproduced on 8½- x 11-inch paper. The electronically generated form must contain all data elements and follow exact format of the existing printed form. The form number of the electronically generated form will be shown as DA Form 5513-R-E and the date will be the same as the date of the current edition of the printed form. A copy for reproduction purposes is located at the back of this handbook. When not in use, the key control register will be kept in a locked container that does not contain or store classified material and to which access is controlled. Keys and combinations to locks for AA&E storage facilities, arms racks, IDS (operational or maintenance), or key containers will not be removed from the installation except to provide for protected storage elsewhere. Keys to locks securing key containers will be afforded physical protection equivalent to that provided by the key container itself. Keys to AA&E storage buildings, rooms, racks, containers, and IDS will be maintained separately from other keys, and accessible only to those individuals whose official duties require access to them. A current roster of these individuals will be kept within the unit, agency, or organization. The roster will be protected from public view. The roster will be signed by the designated official and contain the names of those individuals authorized to receive keys from the key custodian. (See *c* below). At no time will keys be in the custody of a person not listed on the roster. A key control register will be maintained at the unit level to ensure continuous accountability for keys, ensure positive control of keys, and establish responsibility for the custody of stored AA&E. Key control registers will contain printed name and signature of the individual receiving the key, date and hour of issuance, serial number or other identifying information of the key, printed name and signature of the person issuing the key, date and hour key was returned, and the printed name and signature of the individual receiving the returned key. Completed key control registers will be retained in files for a minimum of 90 days and then disposed of per established MACOM procedures.

*b.* Keys to AA&E storage buildings, rooms, racks, containers, and IDS may be secured together in the same key container. However, keys required for maintenance and repair of IDS, including keys to the control unit door and monitor cabinet, will be kept separate from other operational IDS keys and access permitted only to authorized maintenance personnel. Under no circumstances will IDS or AA&E keys or locks, or alternate keys or locks be placed in any security container that contains or stores classified material.

(1) When arms and ammunition are stored in the same areas, keys to those storage areas may be maintained together, but separately from other keys that do not pertain to AA&E storage. The number of keys will be held to the minimum essential. Keys may not be left unattended or unsecured at any time.

(2) When not attended or being used keys will be stored in containers of at least 20-gauge steel or material of equivalent strength, and equipped with GSA-approved low (secondary) security padlocks or GSA-approved built-in 3-position changeable combination locks, or in Class 5 or Class 6 GSA-approved, 3 position, changeable combination container that do not contain or store classified material. Combinations will be recorded on SF 700 (Security Container Information), sealed in the envelope provided, and stored in a container per AR 380-5, chapter 5. Keys and combinations to locks will be accounted for at all times. Key containers weighing less than 500 pounds will be fastened to the structure with bolts or chains equipped with secondary padlocks to preclude easy removal.

(3) In the event of lost, misplaced, or stolen keys, an investigation will be conducted immediately.

The affected locks or cores to locks will be replaced immediately. Replacement or reserve locks, cores, and keys will be secured to preclude access by unauthorized individuals. The use of a master key system or multiple key system is prohibited.

*c.* A key and lock custodian, where duties include assuring proper handling of keys and locks, will be appointed in writing. Only the commander and the key custodian (or alternate, if appointed) will issue and receive keys to and from individuals on the key access roster (*a* above). Personnel listed on the roster may transfer custody, in writing, among themselves. The key and lock custodian's duties will also include procurement and receipt of keys and locks, and investigation of lost or stolen keys. The key and lock custodian will maintain a record to identify each key and lock and combinations to locks used by the activity, including replacement or reserve keys and locks. The record will show the current location and custody of each key and lock. The key and lock custodian(s) will ensure that individuals who are designated to issue, receive, and account for keys in their absence, clearly understand local key control procedures. The key and lock custodian will maintain a key control register at all times to ensure continuous accountability for keys of locks used to secure AA&E.

*d.* Padlocks will be locked to the staple or hasp when the area of container is open to preclude theft, loss, or substitution of the lock.

*e.* Padlocks and their keys will be inventoried by serial number semiannually. Padlocks and keys which do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate. The inventory records will be retained in unit files for a minimum of 1 year and then disposed of per established MACOM procedures. A key and lock inventory will contain a record of keys, locks, key serial numbers, lock serial numbers, location, and the number of keys maintained for each lock. This record will be secured in the key depository.

*f.* When individuals are charged with the responsibility for safeguarding or otherwise having keys immediately available, they will sign for a sealed container of keys. A sealed container is a locked and sealed key container, or a sealed envelope (SF 700 per AR 380-5, paragraph 5-104) containing the key or combination to the key container. When the sealed container of keys is transferred from one individual to another, the unbroken seal is evidence that the keys have not been disturbed. The seal need not be broken for inventory of keys. However, evidence of tampering with a sealed container will require an inventory of the keys and such other action as may be required by the commander concerned. If the keys are not placed in a sealed container, an inventory of keys will be made by serial number or other identifying information of the key (e.g., stamped number on key). The inventory and change of custody will be recorded on the DA Form 5513-R. See paragraph 2-12, for requirements to determine reliability of personnel authorized to issue and control keys to arms and category I and II ammunition and explosives storage facilities.

*g.* Combinations to locks on vault doors or GSA approved Class 5 or Class 6 security containers will be changed annually or upon change of custodian, armorer, or other person having knowledge of the combination, or when the combination has been subject to possible compromise. Combinations will also be changed when a container is first put into service. The combination will be recorded using SF 700, sealed in the envelope provided, and stored in a container meeting storage requirements per AR 380-5, chapter 5. No other written record of the combination will be kept. Controls will be established to ensure that the envelopes containing combinations to locks or containers are not made available to unauthorized personnel.

*h.* Replacement of lock cylinders and broken keys for high security locks may be requested through normal supply channels. Requests will be coordinated through the key control custodian. MACOMs are designated as approval authorities for any deviation in key procurement procedures.

## Chapter 4, Protection of Arms

### 4.1 General

This chapter prescribes the criteria and standards for the protection of arms in custody of DA Components, COE drawing DEF 141-90-04 depicts arms storage room construction meeting the criteria and standards prescribed by this regulation. Arms, including firearms in rod and gun club facilities, will be stored in an arms room, modular vault, or an

arms storage building per the requirements of this chapter.

*a.* When storage in an arms storage room, modular vault, or building will impede training or operational requirements, arms may be stored or installed on the naval craft, vehicle, or aircraft to which assigned or in other configurations per this regulation and as specified by HQDA. Specific guidance issued by HQDA (DAMO-ODL) will be furnished the Deputy Under Secretary of Defense for Policy (DUSDP) within 90 days. Weapons stored or installed in tanks, vehicles, or aircraft will be protected as part of the overall system in which they are stored or installed.

(1) Commanders will establish appropriate security measures to ensure weapons stored or installed in tanks, vehicles, or aircraft are protected at all times, particularly when tanks, vehicles, or aircraft are unmanned. The following guidance applies:

(a) When not in use, tanks, vehicles, or aircraft containing weapons will be parked inside a secure motor pool or an aircraft park area. Level III security III security measures in AR 190-51, paragraphs 3-3 and 3-5, apply.

(b) When operational readiness permits, weapons mounted on tanks, vehicles, or aircraft that are accessible and easily removable will be dismounted and secured inside the locked tank, vehicle, or aircraft, or other secure location. Weapons that are dismounted and secured inside the locked tank, vehicle, or aircraft and weapons that remain installed on board, will be made inoperative by removal of barrels or other essential firing components. Such components will be secured in a locked metal container inside the tank, vehicle, or aircraft, or other secure location. The container will be secured to the tank, vehicle, aircraft, or other secure structure with bolts or chains equipped with secondary padlocks. Spare barrels may be stored inside a locked, totally enclosed armored combat vehicle when the other essential firing components are secured in an arms storage room and the vehicle is parked inside a motor park which provides continuous surveillance by guards and Level III security measures per AR 190-51, paragraph 3-3 and 3-5.

(c) Weapon systems that are impractical to dismount, due to operational readiness or damage to the weapon system will be made inoperable by the removal of essential component or components. Such components will be secured as in (*b*) above. Electrical power may be considered an essential component on the 20MM and 30MM weapon systems.

(d) When electrical power is the only essential component removed from the weapons systems, ammunition for those weapons systems will not be stored on board the tank, vehicle, or aircraft. Level II security measures per AR 190-51, paragraph 3-3 and 3-5 apply.

(2) Large weapons (e.g., crew served weapons and mortar tubes) that cannot be secured in arms rooms, or other arms storage facilities, because of inadequate storage space, may be stored in a locked, totally enclosed armored vehicle. In such cases, security requirements in (1) above apply.

(3) Large weapons that cannot be secured in arms rooms, as stated above, may also be secured in other secure locations, such as a room made secure by compensatory measures. In such cases, protection and surveillance by guard or other personnel will be provided according to the risk category of the weapons involved. Such weapons will be rendered inoperable according to the requirements prescribed in (*b*) above.

(4) During maintenance support operations, weapon components may be stored in a storage facility meeting security requirements according to the risk category of the items involved.

(5) MACOM commanders may authorize storage of small quantities of Category IV arms in a GSA approved Class 5 security containers not storing classified documents or materials without IDS, security lighting, and security patrol requirements. MACOMs will decide the number to be stored on the basis of mission and operational requirements in conjunction with an assessment of vulnerability and threat conditions. Provisions of above apply only to small units (e.g., USACIDC detachment) that must store a small quantity of prescribed weapons for operational requirements.

*b.* Individuals issued, or in possession of arms, are responsible for security of this property while it is entrusted to their care.

(1) Each weapon issued for training, operations, or any other reasons will be carried on the person of the individual to whom issued at all times or it will be properly safeguarded and secured. Except during emergencies, weapons will not be entrusted

to the custody of any other person except those responsible for the security of operational weapons. These persons will comply with issue and turn-in procedures. Local procedures will be established to secure and account for the weapons of personnel medically evacuated during training.

(2) During field exercises and training, pistols and revolvers issued to persons will be secured to the person by either a locally made lanyard or military issued field lanyards (NSN 8465-00-965-1705).

(3) Pistols or revolvers that lack a device to affix the lanyard will be secured by running the lanyard through the pistol/revolver trigger guard during field and training exercises when drawing the pistol/revolver is not contemplated. If drawing the pistol/revolver is contemplated, such pistols/revolvers are exempt from the lanyard requirements.

(4) Pistols and revolvers issued for operational purposes need not be secured by a lanyard except where specified in other regulations.

(5) Local commanders will prescribe specific accountability and security measured to prevent the loss of other weapons assigned to persons.

(6) USACIDC may authorize individuals to retain their assigned weapons in their private quarters if the necessity is dictated by operational requirements. In such instances, USACIDC will establish accountability safeguards and security measures.

4-2. Storage and supplemental controls

*a.* Storage and supplemental controls.

(1) New facilities built for storage of Category II arms will meet the facility criteria in appendix G.

(2) An existing facility in which Category II, III, and IV arms are stored together will meet the criteria for facilities storing Category II arms in appendix G unless the MACOM commander determines it to have equivalent or better security.

(3) Category II arms stored in arms storage buildings or rooms that do not meet or exceed the criteria for Category II arms may be stored in GSA approved Class 5 security containers not containing classified documents or materials, or in a safe-type steel file container not containing classified documents or materials, having a 3-position, dial-type, combination lock providing forced entry protection as approved by GSA (Federal Specification AA-F-363B, as amended) or in approved modular vaults not containing classified documents or materials with GSA approved Class 5 vault doors or GSA approved Class 5 armory doors. Modular vaults meeting Federal Specification AA-V-2737 may be used to meet this requirement. Vaults, containers and safes will be under 24 hour armed guard surveillance or protected by an approved IDS and the facility will be checked by a security patrol at least once every 8 hours.

(4) Category III and Category IV arms will be stored in facilities meeting or exceeding the criteria in appendix G.

(5) Categories III and IV arms that are stored in facilities that do not meet or exceed the criteria for Categories III and IV arms may be stored in a GSA approved Class 5 security container, not containing classified material or documents, or a safe-type steel file cabinet not containing classified material or providing forced entry protection as approved by GSA (Federal Specification AA-F-363B, as amended). Containers weighing less than 500 pounds will be secured to the structure.

(6) Category IV arms that are stored in unmanned facilities not equipped with an IDS will be checked by a security or guard patrol at irregular intervals not to exceed 24 hours.

*b.* Rescinded.

*c.* Arms racks and storage containers.

(1) When not in use, arms will be stored in banded crates, metal containers, approved standard issue racks or locally fabricated arms racks, and secured in approved weapons storage facilities. Standard issue approved metal wall lockers or metal cabinets may be used. Crates or containers will be banded, locked, or sealed in a way that will prevent weapon removal without leaving visible signs of tampering. Screws or bolts used in assembling containers, lockers, or cabinets will be made secure to prevent disassembly.

(2) All arms racks or containers will be locked with approved secondary padlocks. In facilities that are not manned 24 hours a day, rifle racks and containers weighing less than 500 pounds will be fastened to the structure (or fastened together in groups totaling more than 500 pounds) with bolts or with chains equipped with secondary padlocks.

Bolts used to secure racks will be spot welded, brazed, or peened to prevent easy removal. Chains used to secure racks (and containers) will be heavy duty hardened steel, welded, straight links steel, galvanized of at least 5/16-inch thickness, or of equivalent resistance to force required to cut or break a secondary padlock.

(3) Hinged locking bars for racks will have the hinge pins welded or otherwise secured to prevent easy removal. Locally fabricated racks will provide, at a minimum, security equivalent to standard issue racks. All racks will be so constructed as to prevent the removal of a weapon by disassembly. Locally fabricated arms racks will provide protection from forced entry equip to the M12 rack (M-16 rifle rack). Technical data package (TDP) sketches and assembly instructions for local fabrication of arms racks may be requested from CDR, U.S. Army Armament, Munitions and Chemical Command, ATTN: AMSMC-MAG-SS, Rock Island, IL 61299-6000. The local engineer will certify that locally fabricated arms racks are constructed according to TDP specifications and drawings. The engineer certification will serve as security verification for adequacy of such racks. The certification will be maintained on file in the location where such racks are used.

(4) When weapons are in transit, stored in depots or warehouses or held for contingencies, the weapons crates or containers need not be fastened to the structure. However, such crates or containers will be banded or locked and sealed in a way that will prevent weapon removal without leaving visible signs of tampering. The facilities and buildings in which these weapons are stored will meet the structure and other security requirements of this regulation. Arms being unpacked or packed for shipping, or in assembly-line configuration in a maintenance repair or rebuild facility, do not require storage in racks or containers. However, the facilities in which they are stored will meet the structure and other security requirements of this regulation.

*d.* Security lighting.

(1) Interior and exterior lighting will be provided for all arms storage buildings, buildings in which arms storage rooms are located, and arms storage rooms. The lighting will be sufficient to allow guards (or individuals responsible for maintaining surveillance) to see illegal acts such as forced entry, or the unauthorized removal of arms during hours of reduced visibility.

(2) Areas appropriate for lighting include entrances to buildings, corridors, and arms rooms. When an arms room is located inside a building, the entrance door to the arms room will be illuminated. Arms rooms that are located within another room (for example, supply room), do not require security lighting over the arms room door. When an arms room is located inside another secured room, the exterior door to that room will be illuminated.

(3) Security lighting will also be provided for motor pools, hangars, and outdoor parking areas for vehicles or aircraft that have weapons installed or stored on board.

(4) Switches for exterior lights will be installed so that they are not accessible to unauthorized individuals.

(5) Exterior lights will be covered with wire mesh screen, or equipped with vandal resistant lenses, that will prevent the lights from being broken by thrown objects.

*e.* Doors, locks, and locking devices.

(1) Except for GSA approved Class 5 steel vault doors with built-in, three position, changeable combination locks, doors used for access to arms storage rooms or structures will be locked with an approved high security locking device or high security padlock and hasp providing comparable protection to the locks. An approved high security shrouded hasp will be used to secure Category I and II AA&E storage facilities to enhance their security. Doors used for access to arms storage rooms will be locked with approved locks and hasps. On existing storage facilities equipped with double-door protection, high security padlocks and hasps will be used on the most secure door. Secondary padlocks will be used to secure the other door of the double-door concept. Other doors that cannot be secured from the inside with locking bars or dead bolts will be secured on the inside with approved secondary padlocks, e.g., issue window or portals. When high security hasps are installed, locking bars and T-pins should be left in place to aid in opening and closing doors and prevent any future misalignment of the hasps. Panic hardware, when required, will be installed to prevent opening the door by tampering from the outside. Panic hardware will meet safety, fire, and building codes and be approved by the

Underwriters Laboratory or host country requirements as applicable.

(2) Key and lock controls will be established per paragraph 3-8.

(3) Facilities in which vehicles or aircraft are stored with sensitive items aboard will be secured by approved secondary padlocks. Aircraft will be secured with manufacturer-installed or approved modification work order door-locking devices when not in use. All hatches and other openings to track vehicles which cannot be secured from the inside will be secured from the outside with approved secondary padlocks.

*f.* Additional controls.

(1) IDS for arms storage facilities. Arms room storing Category II arms, GSA-approved Class 5 Weapons Storage Cabinets, and GSA approved security modular vaults will be provided with an approved IDS. Facilities without an operational IDS require constant surveillance by an armed guards for Category II arms while Category III and IV facilities require only constant surveillance. In the event that the arming of guards off a military installation is prohibited by State or territorial law, a request for exception to this requirement according to paragraph 2-4 is required. The exception will include the rationale and justification for not utilizing armed guards and the compensatory security measures taken.

(2) Security patrols.

(a) Facilities will be checked by a security patrol periodically as dictated by any threat and by the vulnerability of the facility. For Category II IDS protected facilities, the intervals between checks will not exceed 8 hours. For Category III and IV facilities, the intervals between checks will be once every 24 hours and once every 48 hours for IDS protected storage facilities.

(b) Facilities storing arms outside a military installation will be checked by a security patrol on an irregular basis at an interval not to exceed 24 hours.

(3) Rendering weapons inoperable. If the facility is not located on a military installation, weapon will be rendered inoperable by the method shown in table 4-1 under any of the conditions below:

(a) A facility does not meet structural criteria.

(b) A threat is received.

(c) An IDS is inoperative for a period of 24 hours or longer.

(d) During periods of annual field training, if arms are left in the facility.

(e) Decision of the commander having direct security responsibility for the facility.

(4) Storing removed items. The item(s) removed for the purpose of rendering a weapon inoperable will be tagged with the weapons serial number to ensure return to the same weapon and secured in a separate building. Etching of weapon's serial number on the removed parts is prohibited. The removed items will be stored in a locked container in a secure area away from the arms storage facility. If a secure area is not available for separate storage of these items, the container will be stored in the arms storage facility and secured to the structure with an approved lock and chain or equal methods when the container weighs less than 500 pounds.

**Table 4-1. Methods for rendering Small Arms inoperable.**

| |
|---|
| **Weapon:** Carbine, Caliber .30 M1<br>**Method:** Remove bolt assembly |
| **Weapon:** Gun, Auto 25mm M242<br>**Method:** Remove bolt and track assembly |
| **Weapon:** Launcher, grenade 40mm M79<br>**Method:** Remove barrel assembly |
| **Weapon:** Launder, grenade 40mm M203<br>**Method:** Remove barrel assembly |
| **Weapon:** MG, Caliber .50 M2 series<br>**Method:** Remove bolt assembly |
| **Weapon:** MG, 7.62mm M60 series |

**Method:** Remove breech block

---

**Weapon:** MG, 7.62mm M73 series
**Method:** Remove breech block

---

**Weapon:** MG, Caliber .50 M85
**Method:** Remove bolt assembly

---

**Weapon:** MG, 7.62mm M219
**Method:** Remove Breech block

---

**Weapon:** MG, 7.62mm M240 series
**Method:** Remove bolt and operating rod assembly

---

**Weapon:** MG, 5.56mm 249
**Method:** Remove bolt and slide assembly

---

**Weapon:** MG, 40mm MK19 Mod 3
**Method:** Remove bolt assembly

---

**Weapon:** Pistol, semi-auto, Caliber .45 M1911A1
**Method:** Remove firing pin and spring. Leave stop installed to prevent damage of firing pin hold

---

**Weapon:** Pistol, semi-auto, Caliber .22
**Method:** Remove bolt or slide assembly

---

**Weapon:** Pistol, semi-auto, 9mm M9
**Method:** Remove firing pin assembly, recoil spring, and the spring guide from the spring assembly

---

**Weapon:** Rifle, Caliber .22--all types
**Method:** Remove bolt assembly

---

**Weapon:** Rifle, Caliber .30 M1 series
**Method:** Remove bolt assembly

---

**Weapon:** Rifle, 7.62mm M14 series
**Method:** Remove bolt assembly

---

**Weapon:** Rifle, 5.56mm, M16 series
**Method:** Remove firing pin

---

**Weapon:** Rifle, Caliber .30 M1918
**Method:** Remove firing pin series

---

**Weapon:** Shotgun, 12 gauge, riot type
**Method:** Remove barrel assembly

---

**Weapon:** Sub MG, Caliber .45 M1 series
**Method:** Remove bolt assembly

---

**Weapon:** Sub MG, Caliber .45 M3 series
**Method:** Remove bolt assembly

---

**Weapon:** Sub MG, 5.56mm M231
**Method:** Remove firing pin

---

**Weapon:** Recoilless rifle, 90mm M67
**Method:** Remove breech block

---

**Weapon:** Revolver, Colt
**Method:** Remove cylinder and crane assembly

---

**Weapon:** Revolver, Ruger
**Method:** Remove strut assembly

---

**Weapon:** Revolver, Smith and Wesson
**Method:** Remove cylinder and yoke assembly

---

*g.* RC weapons. The Army policy of close cooperation between Active Army and RC activities is an essential element in eliminating the theft or loss of AA&E. At times, RC activities may need to use local Active Army facilities for the temporary storage of AA&E as the result of emergency situations; for example, during vehicle breakdown when transporting weapons, when an increased threat situation is forecast or present, and during rifle matches. Active Army facilities are authorized and encouraged to assist in temporarily securing RC items. However, the receiving unit will ensure the accountability (number and type items, including serial numbers) of those items accepted for storage. The above policy also applies between Reserve components as well as the temporary storage of Active Army stocks at Reserve storage facilities.

4.3 Storage of classified weapon trainers

Because of security classification, nuclear weapon trainers or other classified weapon trainers may be stored in separate locked containers, or wire cages, in arms storage facilities when alternate facilities are not available per AR 380-5, chapter 5. Commanders will prescribe supplementary measures and controls to prevent unauthorized access and ensure the items are accounted for at all times.

4-4. Consolidated arms rooms

Arms belonging to more than one unit or organization may be stored in the same arms room or arms storage facility. Arms will be identified by unit. One commander will be designated as having responsibility for the overall security of the consolidated storage facility. Access controls will be established to ensure protection of each unit's arms. Procedures will also be established to fix responsibility for issue, receipt, and physical accountability for arms, including ammunition, and all other sensitive items, stored in the consolidated storage facility, per AR 710-2, paragraph 2-12; and DA Pam 710-2-1, paragraph 9-11. Where feasible, unit arms will be separated by secondary padlocks. If this is done, each unit will maintain sensitive items. Units with small quantities of arms may use locked metal containers instead of separation by partitions. In all cases, one designated commander will continue to have responsibility for the overall security of the consolidated storage facility, including access to that facility. COE drawing DEF 33-33-18 depicts a consolidated arms storage building meeting this criteria. COE drawing STD 40-21-01 depicts expanded metal mesh security cage. Units will provide the commander respon-sible for the overall security of the consolidated storage facility. Procedures for such consolidated arrangements will be established in SOP of the consolidated storage facility, or in the SOP of the higher headquarters.

4.5 Privately-owned weapons and ammunition

*a.* Commanders will ensure privately-owned arms and ammunition (including authorized war trophies) are protected on their installations and facilities. Based upon local requirements and availability of resources, Commanders may establish and maintain a system for the registration of privately owned arms on their installations. Commanders will--

(1) Secure arms and ammunition in the installation armory or unit arms rooms in approved locked containers separate from the military AA&E. Storage requirements in this regulation apply. Installation commanders may authorize storage of these items in other locations on military installations, provided they are properly secured.

(2) Account for and inventory arms and ammunition.

(a) A DA Form 3749 (Weapons Receipt) will be issued for each privately-owned weapon secured in the arms rooms.

(b) Privately-owned weapons will be inventoried in conjunction with, and at the frequency of the inventory of Government weapons.

(c) Commanders will establish limits on the quantity and type of privately owned ammunition

stored in the arms room, based upon availability of space and safety considerations.

(3) Post applicable local regulations and State and local law information on ownership, Registration, and possession of weapons and ammunition on unit bulletin boards.

(4) Conduct inspections per AR 190-13, paragraph 2-8, and this regulation to ensure proper storage and control.

(5) Process unauthorized AA&E per AR 190-22, paragraph 3-4.

(6) Prohibit retention and storage of incendiary devices and explosives.

(7) Brief all newly assigned persons on this regulation and subordinate command guidance. All personnel will be made aware of changes.

*b.* Personnel keeping or storing privately owned arms and ammunition (including authorized war trophies) on military installation will:

(1) Comply with local regulations and local and State laws on ownership, possession, registration, off-post transport, and use.

(2) Store both arms and ammunition in the unit arms room or other locations authorized by the installation commander.

(3) Follow local security and safety regulations. Safeguard the unit issued DA Form 3749 for turn-in to the unit armorer when the weapon is withdrawn from the arms room.

(4) Withdraw privately-owned weapons and ammunition from the unit arms rooms only upon approval of the unit commander or the commander's authorized representative.

(5) Ship or store arms and ammunition as personal property, if authorized, per AR 55-355, paragraph 50-12. When loss occurs, notify the local provost marshal or security officer immediately.

(6) Comply with the National Firearms Act of 1968 when receiving or bringing arms into the United States. Automatic arms must be turned over to the Bureau of Alcohol, Tobacco and Firearms (BATF), or brought under Army control.

## Appendix B
## Sensitive Arms, Ammunition, and Explosives (AA&E) Security Risk Categorization

### B-1. Application

The requirements of this regulation apply only to rounds of 40mm and larger, conventional, guided missile and rocket ammunition weighing 100 pounds or less per round, and 1,000 or more rounds of ammunition smaller than 40mm. Blank ammunition, .22 caliber rimfire ammunition, and inert training ammunition are excluded from the requirements of this regulation. Further, artillery, tank, mortar ammunition, 90mm and larger are excluded from the requirements of this regulation.

*a.* On the basis of their relative utility, attractiveness, and availability to criminal elements, all AA&E will be categorized according to the risks involved. As a general rule, only arms, missiles, rockets, explosive rounds, mines, and projectiles that have an unpacked unit weight of 100 pounds or less will be categorized as sensitive for purposes of this regulation. Any single container that contains a sufficient amount of spare parts that, when assembled, will perform the basic function of the end item will be categorized the same as the end item.

*b.* The categories of missiles, rockets, and arms will be as stated in paragraph B-2. Nonnuclear missiles and rockets similar to those listed under Category I will automatically be included in that category as they come into the inventory.

*c.* Identifications, codings, corollary plans, and actions for physical security accountability and transportation pertaining to sensitive conventional arms, rockets, missiles, ammunition, and explosives will be uniform throughout the DOD. These items will be integrated into standard catalog data by all services and will be included in applicable documents that address physical security, accountability, storage, transportation, and other related functional activities. The JOCG through tri-service coordination, will use the Decision Logic Formulas (tables B-1 to B-6), and will determine the appropriate categories for ammunition and explosives items. Those responsible for the physical security of facilities storing AA&E will look up the assigned categories in the Army Master Data File (AMDF). Examples of sensitive ammunition and explosive items are shown in paragraph B-2.

*d.* To ensure a uniform approach to sensitive item identification and coding, AMC will incorporate the criteria into their respective cataloging policies and procedures. The criteria will also become a part of the federal cataloging system. Sensitive AA&E items are identified by the controlled item codes per AR 708-1, chap 7. These codes indicate the controls required for storing and transporting each category of AA&E and are listed in the AMDF.

The AMDF is the official source of current security risk codification of all sensitive AA&E items. Codes assigned to specific AA&E items are shown in the monthly AMDF near the center of the microfiche under the column "(CIIC)." The AMDF microfiche for AA&E, and Catalog Data Activity (CDA) Pamphlet 18-1, Code Reference Guide, are available upon request from Chief, U.S. Army Materiel Command, Catalog Data Activity, ATTN: AMXCA-DL, New Cumber-land Army Depot, New Cumberland, PA 17070-5010. The basic responsibility for the assignment and correction of the codes rests with the designated data proponent. Per AR 708-1, chapter 5, U.S. Army Armament, Munitions, and Chemical Command is primarily responsible for materiel management for weapons and ammunition; U.S. Army Missile Command is primarily responsible for materiel management of large rockets and guided missiles per AR 708-1, chapter 5. Further information or assistance regarding security risk codification may be obtained by contacting the AMC Logistics Assistance Offices which are located at selected installations Army-wide.

*e.* AMC will revise, as appropriate, ammunition and explosives codings by means of routine catalog data changes. The exception to applying the methodology in *c* above shall be when tri-Service agreement is reached on a case-by-case basis to place an item in a higher or lower security risk category than that indicated by the total numerical value.

**B-2. Representative risk categories**

*a. Category I (missiles and rockets).*

(1) Nonnuclear manportable missiles and rockets "in a ready to fire" configuration; for example, Hamlet, Redeye, Stinger, Dragon, Javelin, light antitank weapon (LAW) and Viper. The AT-4 antitank weapon is also included.

(2) This category also applies where the launcher tube and the explosive rounds are jointly stored or transported.

*b.* Arms.

(1) Category II. Light automatic weapons, including .50 caliber, M16A2 rifle, Squad Automatic Weapon (SAW), and 40mm MK 19 machine gun.

(2) Category III.

(a) Launch tube and gripstock for Stinger missile.

(b) Launch tube, sight assembly, and gripstock for Hamlet and Redeye missiles.

(c) Tracker for Dragon missiles.

(d) Mortar tubes up to and including 81mm.

(e) Grenade launchers.

(f) Rocket and missile launchers, unpacked weight of 100 pounds or less.

(g) Flame throwers.

(h) The launcher or missile guidance set or the optical sight for the ground mounted TOW.

(i) Launch control unit for Javelin missile.

(3) Category IV.

(a) Shoulder-fired weapons, other than man-portable missiles, rockets, and grenade launchers, not fully automatic.

(b) Handguns.

(c) Recoilless rifles, including 90mm.

*c.* Ammunition and explosives.

(1) Category I. Explosive complete rounds for Category I missiles and rockets(See *a*(1) above).

(2) Category II.

(a) Hand or rifle grenades, high explosive, and white phosphorus.

(b) Mines, antitank, or antipersonnel (unpacked weight of 50 pounds or less each).

(c) Explosives used in demolition operations; for example, C-4, military dynamite, and TNT.

(d) Critical binary munitions components containing "DF" and "QL" when stored separately from each other and from the binary chemical munition bodies in which they are intended to be employed (See AR 50-6-1, chap 5 and app D, Chemical Agency Security Program, for security requirements of other chemical agents).

(3) Category III.

(a) Ammunition, .50 caliber and larger, with explosive filled projectile (unpacked weight of 100 pounds or less each).

(b) Grenades, incendiary, and fuzes for high explosive grenades.

(c) Blasting caps.

(d) Supplementary charges (uninstalled, or installed in projectiles in a manner allowing easy removal without special tools or equipment).

(e) Bulk explosives.

(f) Detonating cord.

(4) Category IV.

(a) Ammunition with nonexplosive projectile (unpacked weight of 100 pounds or less each).

(b) Fuzes, except for (3)(*b*), above.
(c) Grenades, illumination, smoke, and CS/CN (tear producing).
(d) Incendiary destroyers.
(e) Riot control agents, 100 pound package or less.
(f) Ammunition for weapons in (3), above, not otherwise categorized.

**Table B-1. Decision Logic Formulas (DLFs).**

**Factor:** 1
**Utility:** High
**Casualty/Damage Effect:** High
**Adaptability:** Without modification
**Portability:** Easily carried or concealed by one person.

**Factor:** 2
**Utility:** Moderate
**Casualty/Damage Effect:** Moderate
**Adaptability:** Slight modification
**Portability:** Can be carried by one person for short distances.

**Factor:** 3
**Utility:** Low
**Casualty/Damage Effect:** Low
**Adaptability:** Major modification
**Portability:** Requires at least two persons to carry.

**Factor:** 4
**Utility:** Impractical
**Casualty/Damage Effect:** None
**Adaptability:** Impractical
**Portability:** Requires materials handling equipment (MHE) to move.

**Table B-2. Risk Factors--Utility.**

**Risk Factor:** 1
**Utility:** High
**Description:** High explosive, concussion, and fragmentation devices.

**Risk Factor:** 2
**Utility:** Moderate
**Description:** Small arms ammunition.

**Risk Factor:** 3
**Utility:** Low
**Description:** Ammunition items not described above--NONLETHAL, civil disturbance chemicals, incendiary devices.

**Risk Factor:** 4
**Utility:** Impracticable
**Description:** Practice, inert, or dummy munitions; small electric explosive devices; fuel thickening compound; or items possessing other characteristics which clearly and positively negate potential use by terrorist, criminal, or dissident functions.

**Table B-3. Risk Factors--Casualty/Damage Effect.**

**Risk Factor:** 1
**Casualty/Damage Effect:** High
**Description:** Extremely damaging or lethal to personnel; devices which will probably cause death to personnel or major material damage.

**Risk Factor:** 2
**Casualty/Damage Effect:** Moderate
**Description:** Moderately damaging or injurious to personnel; devices which could probably cause personnel injury or material damage.

**Risk Factor:** 3
**Casualty/Damage Effect:** Low
**Description:** Temporarily incapacitating to personnel.

**Risk Factor:** 4
**Casualty/Damage Effect:** None
**Description:** Flammable items and petroleum based products readily obtainable from commercial sources.

**Table B-4. Risk Factors--Adaptability.**

**Risk Factor:** 1
**Adaptability:** Without
**Description:** Unusable as is; simple to function without modification use of other components.

**Risk Factor:** 2
**Adaptability:** Slight Modification
**Description:** Other components required; or can be used with slight modification.

**Risk Factor:** 3
**Adaptability:** Major Modification
**Description:** Requires the use of other components which are not available on the commercial market; or can be used with modification that changes the configuration.

**Risk Factor:** 4
**Adaptability:** Impracticable
**Description:** Requires specified functions or environmental sequences which are not readily reproducible, or construction makes it incapable of producing high order detonation; for example, gas generator grains, and impulse cartridges.

**Table B-5. Risk Factors--Portability.**

**Risk Factor:** 1
**Adaptability:** High
**Description:** Items which easily can be carried by one person and easily concealed.

**Risk Factor:** 2
**Adaptability:** Moderate
**Description:** Items whose shape, size, and weight allows them to be carried by one person for a short distance.

**Risk Factor:** 3
**Adaptability:** Low
**Description:** An item whose shape, size, and weight requires at least two persons to carry.

**Risk Factor:** 4
**Adaptability:** MHE Required
**Description:** The weight, size, and shape of these items preclude movement without MHE.

**Table B-6. Computation of risk factor numerical values (1).**

**Evaluation:** High Sensitivity
**Numerical Values of Risk Factors:** (4-5)
**Physical Security Risk Category Code:** II

**Evaluation:** Moderate Sensitivity
**Numerical Values of Risk Factors:** (6-8)
**Physical Security Risk Category Code:** III

**Evaluation:** Low Sensitivity
**Numerical Values of Risk Factors:** (9-12)
**Physical Security Risk Category Code:** IV

NOTES:
1. AMC shall use the logic formula in table B-1, to determine the numerical values and the physical security risk category codes as shown above. (Use only one factor value for each column and total the numbers for each column to obtain the security risk category.)

## Appendix F
## Specification for Intrusion Detection System Signs

**F-1.** A sample intrusion detection system sign that may be used is shown below in figure F-1. The sign is flat with shape, size, and legend as shown. The sign face should consist of reflectorized sheeting bonded to an aluminum backing.
**F-2.** Sign backing is flat, degreased, etched, and unpainted aluminum alloy, type 6061T6, not less than 1/16-inch thick. For interior posting, plastic or wood could be used.
**F-3.** In non-English speaking overseas areas, a sign in the language of the host country, should be mounted alongside the English language sign. In U.S. states and possessions where a major minority language is spoken, similar signs may be posted as a safety precaution.

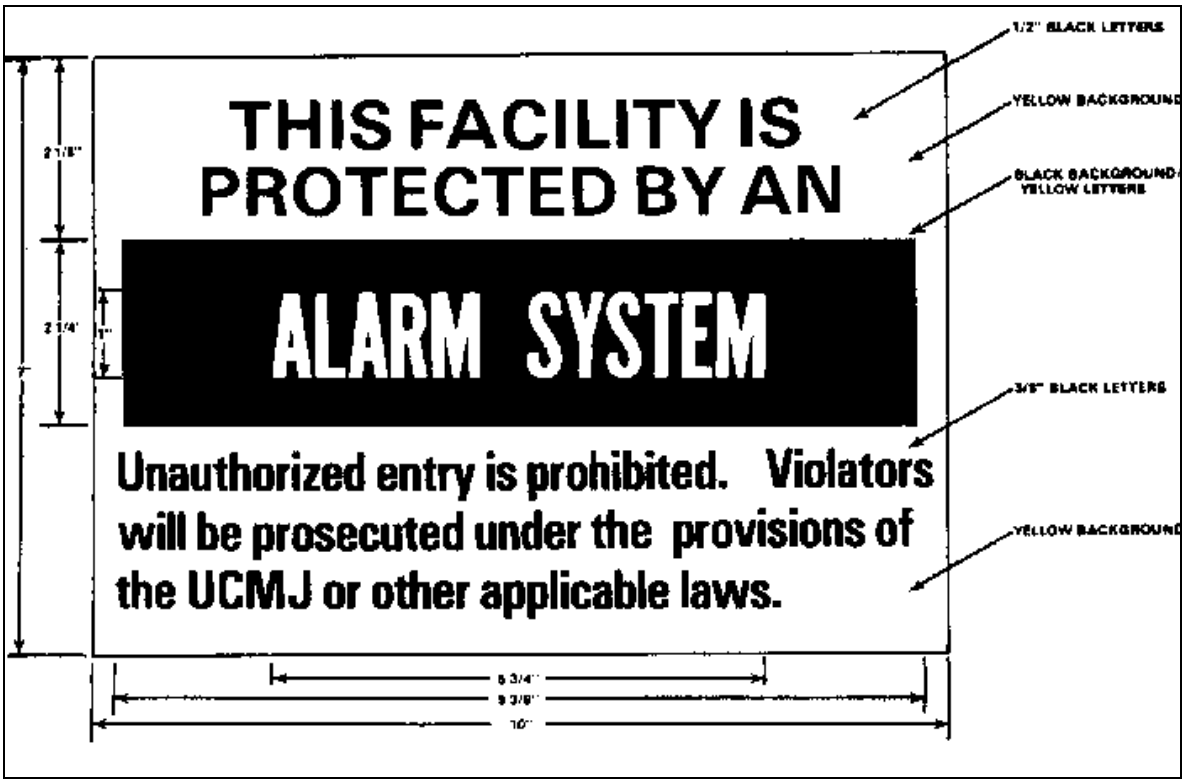



Figure F-1. Sample Intrusion Detection System Sign

*(End of extract of AR 190-11)*

*(Start of extract of AR 190-13)*

Army Regulation 190-13

Military Police

# The Army Physical Security Program

30 September 1993

Effective: 30 October 1993

Unclassified

---

## Chapter 6 Restricted Areas

### 6-1 General

This chapter sets forth guidance on the definition and designation of restricted areas within the 50 United States. Commanders outside the continental United States (OCONUS) may use information in this chapter to set up local procedures according to U.S. and host country agreements.

### 6-2. Authority (summarized)

*a.* Section 793(a), Title 18, United States Code. It is a felony for anyone to obtain information on national defense with the intent, or reason to believe, that such information is to be used to the injury of the United States, or to the advantage of a foreign nation to enter, fly over, or otherwise obtain information about installations, facilities, or places that are connected with the national defense and controlled by the United States.

*b.* Section 793(b), Title 18, United States Code. It is a felony for anyone with like purpose and with like intent, attempts to or does copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense.

*c.* Section 21, Internal Security Act of 1950 (64 Stat. 1005, 50 USC 797). See extract in app C.

### 6-3. Designation of restricted areas

*a.* When conditions warrant, commanders of Army installations will designate restricted areas in writing to protect classified defense information, or safeguard property or material for which they are responsible.

*b.* Tenant units and activities on the installation will request the authority of the installation commander to designate their restricted areas.

*c.* Designation of restricted areas for Army activities not on an installation will be by the authority of the activity commander or officer in charge.

*d.* When required, physical safeguards will be installed to deter entry of unauthorized persons into the restricted area.

*e.* Commanders designating or terminating restricted areas to meet the requirements of AR 380-19, AR 380-40, AR 381-14, or AR 530-4, will advise the Commander, U.S. Army Intelligence and Security Command, ATTN: IAOPS-OP, Fort Meade, MD 20755-5995, of the establishment or termination. The applicable regulation will be cited.

### 6-4. Posting of restricted areas

*a.* Except when such action would tend to advertise an otherwise concealed area, or when in conflict with Host Nation Agreements, signs or notices will be posted in conspicuous and appropriate places to identify a restricted area. This includes signs posted at each entrance or approach to the area, and on perimeter fences or boundaries of the area.

*b.* Failure to post conspicuous signs and notices to give people approaching a restricted area actual knowledge of the restriction, may seriously hamper any resulting criminal prosecution.

*c.* Each sign or notice will be marked with the words,"**RESTRICTED AREA**," and include the warning notice below. **THIS (INSTALLATION, ACTIVITY, ETC.) HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF (TITLE: COMMANDING GENERAL OR COMMANDING OFFICER) IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE ON 20 AUGUST 1954, PURSUANT TO THE PROVISIONS OF SECTION 21, INTERNAL SECURITY ACT OF 1950. UNAUTHORIZED ENTRY IS PROHIBITED. ALL PERSONS AND VEHICLES ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHING OR MAKING NOTES, DRAWINGS, MAPS, OR GRAPHIC REPRESENTATIONS OF THIS AREA OR ITS ACTIVITIES ARE PROHIBITED UNLESS SPECIFICALLY AUTHORIZED BY THE COMMANDER. ANY SUCH MATERIAL FOUND IN THE POSSESSION OF UNAUTHORIZED PERSONS WILL BE CONFISCATED.**

*d.* In areas in which English is but one of two or more languages commonly spoken, warning signs will contain the local languages besides English.

### 6-5. National defense areas

*a.* A restricted area may be established on nonfederal lands within the United States, its possessions or territories, to protect classified defense information, and DOD equipment or material. When this type of area is established, it will be referred to as a National Defense Area (NDA). Examples of a NDA would include

nuclear and chemical event (formerly accident or incident) sites, and aircraft crash sites.

*b.* Establishing a NDA temporarily places such non-federal lands under the effective control of DOD, and results only from an emergency event.

*c.* The senior DOD representative at the scene will define the boundary, mark it with a physical barrier, and post warning signs. Every reasonable attempt will be made to obtain the landowner's consent and cooperation in establishing of the NDA; however, military necessity will indicate the final decision regarding location, shape and size of the NDA.

*d.* The authority to establish a NDA includes the authority to deny access to the NDA. It also includes the authority to remove persons who threaten the orderly administration of the emergency site. Use of force employed to enforce this authority will be in accordance with AR 190-14.

6-6. Restricted area violation procedures

*a.* The Army installation commander will cause any person who enters a restricted area without authority to be brought immediately before proper authority for questioning.

(1) The person may be searched per AR 190-30. Any notes, photographs, sketches, pictures, maps, or other material describing the restricted area may be seized.

(2) Persons brought before proper authority for questioning will be advised of their rights per AR 190-30, appendix C. Questioning will be conducted without unnecessary delay.

*b.* If the person was unaware of the restriction, and neither acquired nor intended to acquire knowledge of sensitive or classified information by entering, that person will be warned against reentry and released.

*c.* If it appears that the person knowingly entered a restricted area, or may have acquired or intended to acquire sensitive or classified information by entering, or may have committed some other offense, the actions below will be taken.

(1) Persons not subject to the Uniform Code of Military Justice (UCMJ) will be taken without delay to civilian law enforcement officials. In the United States, the nearest office of the FBI will be notified, and the person will be turned over to the nearest U.S. Marshal. If the person cannot be turned over to a U.S. Marshal within a reasonable period of time (three or four hours), he or she will be taken before an appropriate state or local official. (See 18 USC 3041.) As soon as possible, the agency to which the person is transferred will be given a written statement of the facts, the names and addresses of the witnesses, and pertinent exhibits as may be available.

(2) A person subject to the UCMJ will be turned over to his or her commander or the proper military law enforcement official.

*d.* Facts regarding a deliberate violation of a restricted area will be immediately reported per AR 381-12, paragraph 8.

***(End of extract of AR 190-13)***

# Student Handout 2

This handout contains an extract of AR 190-51 you will need to study to complete this lesson.

**Military Police**

# Security of Unclassified Army Property (Sensitive and Nonsensitive)

# AR 190-51

**Headquarters**
**Department of the Army**
**Washington, DC**
**30 September 1993**

## Chapter 1
## Introduction

### 1-1. Purpose
This regulation prescribes policies, procedures, and responsibilities for safeguarding unclassified U.S. Army property, both sensitive and nonsensitive. Its policy objectives are to—

a. Establish standardized, minimum acceptable security requirements for specified categories of U.S. Army property.

*b.* Provide a risk analysis method that allows commanders the flexibility to tailor physical security posture and resources to meet local needs.

*c.* Reduce loss, theft, misuse, and damage of Army assets cost effectively.

### 1-2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

### 1-3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the glossary.

### 1-4. Responsibilities
a. Deputy Chief of Staff for Operations and Plans (DCSOPS) will-

(1) Provide overall staff responsibility for the security of unclassified Army property (sensitive and nonsensitive).

(2) Coordinate with the Army Staff (ARSTAF) and major Army commands (MACOMs) to establish policy, procedures, and standards pertaining to security of Army property.

*b.* The Director of Information Systems for Command, Control, Communications, and Computers will resolve any conflicts in U.S. Army policy concerning the control of controlled cryptographic items (CCI).

*c.* Installation commanders, major United States Army Reserve Commands (MUSARC), and state adjutants general (AG) will-

(I) Ensure a risk analysis is conducted for the assets of all assigned and tenant units and activities maintaining specified facilities for particular categories of Army property under this regulation and for any other assets which have been designated mission essential or vulnerable as indicated in Army Regulation (AR) 190-13.

(2) Ensure a risk analysis is conducted for the assets of units and activities which are to occupy new or renovated facilities or facility additions. Risk analyses for assets to be located in such facilities will be performed during the planning stages of the facility construction or renovation so that security measures can be incorporated at the project's inception.

(3) Determine security requirements for museum activities in their commands and comply with this and other related regulations and directives.

*d.* The numbered armies in the continental United States (CONUSA), installation, division, MUSARC, separate brigade commanders, and state AGs, upon declaration of war or when operating in a designated hostile area, may prescribe procedures suspending specific provisions of this regulation to account for local conditions while ensuring maximum practical security for Government personnel and property. This authority may be delegated to commanders in the grade of lieutenant colonel.

*e.* Unit commanders or activity chiefs will control and safeguard all supply and equipment areas within their command or activity. They will-

(1) Promptly report to the provost marshal or equivalent organization, investigate, and resolve incidents involving loss, theft, misuse, or damage of Army resources.

(2) Establish end-of-day security checks using Standard Form (SF) 701 (Activity Security Checklist).

(3) Implement security measures associated with the conduct of risk analysis using this regulation and Department of the Army (DA) Pamphlet 190-51.

(4) Ensure physical security officers are appointed, in writing, to perform, as a minimum, the duties outlined in AR 190-13.

*(5)* Ensure security plans outlining responsibilities and procedures for the proper control and accountability of assets are written and appropriately disseminated.

(6) Ensure assets are secured by approved locking devices (locks, chains, seals, etc.) as outlined in appendix D.

*f* Units, activities, and installations involved in supply operations will protect their own supplies and equipment as indicated in this regulation.

g. Facility commanders will ensure physical security inspections are conducted per AR 190-13. In addition, commanders may request the U.S. Army Criminal Investigation Command (USACIDC) to conduct crime prevention surveys for the purpose of detecting crime, evaluating the possibilities of easy criminal activity, and identifying procedures conducive to criminal activity.

*h.* Commanders and individuals who are assigned custody of controlled medical substances cited in this regulation are responsible for implementing the measures to safeguard them required by this regulation. These responsibilities include:

(1) Ensuring physical security responsibilities are fixed in the receipt, storage, issue, transportation, use, disposal, turn—in, and accounting for all controlled medical substances and sensitive items.

(2) Providing specific security instructions to individuals who are in the possession and control of, or who are responsible for, controlled medical substances and sensitive items.

(3) Ensuring the careful selection of personnel, including volunteer workers, who are assigned duties that require access to controlled medical substances and sensitive items storage areas or who have custodianship or possession of keys and combinations to locks securing these areas.

(4) Taking action to deny access to controlled substances by individuals undergoing investigation, treatment, rehabilitation, judicial or nonjudicial processes, or administrative action as a result of actual or suspected drug abuse or as a result of suspected illegal activity involving controlled drugs (for example, theft, wrongfully prescribing, inventory manipulation, etc.).

(5) Establishing appropriate escort procedures and desiguating escort personnel, by name or duty position, to escort unauthorized people into storage areas.

(6) Ensuring a physical security officer is appointed, in writing, by the medical facility commander to assure that appropriate protection is provided for all controlled medical substances and sensitive items.

*i.* The museum curator is the authority who decides if a weapon is antique or unique and if it should be made inoperable for display purposes.

### 1-5. Security measures and standards
a. Physical security measures or standards more stringent than those contained in this regulation, as appropriate, will be developed jointly by the tenant activity commander, the installation physical security officer, and host installation commander. Such measures will be based on a threat analysis developed from the risk analysis in DA Pam 190-51 using Technical Manual (TM) 5-853-1. These measures will be incorporated into the installation physical security plan as an annex.

*b.* Provisions for security and necessary funding will be included in normal budget documents. Tenant activities must identify their security requirements to the host installation.

*c.* Installation of intrusion detection systems (IDS) will be according to the applicable Office of the U.S. Army Corps of Engineers guide specifications and with applicable Army regulations (to include AR 190-13).

*d.* Provision of security measures beyond those required by this regulation will be per TM 5-853-1.

### 1-6. Waivers and exceptions
*a.* Waivers and exceptions for all unclassified Army property discussed in this regulation will be considered individually.

(1) Requests for waivers and exceptions will be submitted, in

writing, with complete justification and a statement of compensatory measures in effect through command channels and through the MACOM commander or appropriate staff element having staff cognizance to HQDA (DAMO-ODL-S), 400 ARMY PENTAGON, WASH, DC 20310-0400. Waivers will not be granted for periods exceeding 12 months. Exceptions will be regarded as permanent; however, they will be reviewed and revalidated every 2 years by HQDA (DAMO-OL-S), which retains the authority to revoke exceptions.

(2) Requests for waivers or exceptions will be coordinated with the law enforcement activity, provost marshal, or security officer. When structural deficiencies exist, requests also will be coordinated with the supporting Director of Engineering and Housing (DEH) or equivalent organization.

(3) Active and reserve component provost marshals will submit through command channels and their MACOM to HQDA (DAMO-ODL-S) a list of exceptions to physical security requirements and indicate whether the exceptions are to be continued or canceled.

*b.* Waivers and exceptions to the requirements of this regulation will be kept to a minimum.

(1) Authority to grant waivers and exceptions is delegated to HQDA (DAMO-ODL-S).

(2) Requests for waivers and exceptions will include an adequate description of circumstances requiring the action and a description of compensatory measures. Requests will be submitted, in writing, through command channels to HQDA (DAMO-ODL-S) for individual evaluation. Blanket waivers or exceptions are not authorized.

(3) Waivers normally will be valid up to but not to exceed 1 year. A permanent exception from the specific requirements of this regulation will be permitted only under the conditions described below.

**(**a**)** Unique circumstances at a given unit, facility, or installation are such that conformance to the established standards is impossible, highly impracticable, or unnecessary.

*(b)* Security afforded is equal to or greater than that provided by the standard criteria.

## Chapter 2
## Risk Analysis

### 2-1. General

a. To provide the most practical protection for Army assets, commanders must identify the assets to be protected and analyze the risks to those assets from espionage, sabotage, terrorism, damage, misuse, and theft. Analysis of these risks will assist in determining the type and minimum level of protection needed to safeguard the identified resources adequately and economically.

*b.* The objectives of risk analyses are to-

(1) Provide commanders a tool with which to design a physical security system based on local needs.

(2) Allow commanders the flexibility to adapt the use of physical security resources to local risk conditions.

(3) Obtain the maximum security return from invested fiscal and manpower resources.

(4) Serve as a basis for an asset-specific threat analysis.

### 2-2. Use of risk analysis

*a.* The background and explanation of step-by-step procedures for determining security requirements and conducting a risk analysis for categories of Army property are in DA Pam 190-51.

*b.* A risk analysis will be conducted for those installations or facilities that the installation or MUSARC commanders or the State AGs determine mission essential or vulnerable as indicated in AR 190-13 and which include one or more of the categories of U.S. Army property addressed in this regulation. A risk analysis will be conducted on all mission essential and vulnerable areas (MEVAs)-

(1) When a unit or activity is activated.

(2) When a unit permanently relocates to a new site or facility.

(3) When no formal record exists of a prior risk analysis.

(4) At least every 3 years or more frequently at the discretion of the unit or activity commander.

(5) During the planning stages of new facilities, additions to facilities, and facility renovations.

(6) When an incident occurs in which an asset is compromised.

*c.* The risk analysis will be conducted jointly by designated representatives of the installation commander, the using unit or activity, and the supporting installation provost marshal or equivalent security officer representative.

### 2-3. Implementation of risk analysis

a. Based on the risk analysis results, the unit commander or activity chief will implement the physical protective measures and security procedures described in chapters 3, 4, or 5 of this regulation, as appropriate.

*b.* Results of the risk analysis and physical protective measures, security procedural measures, and terrorism counteraction measures to be implemented will be recorded on DA Form 7278-R (Risk Level Worksheet), with all attachments as necessary. Instructions for the use of DA Form 7278-R are in DA Pamphlet 190-51. Copies of these records will be kept by the supporting provost marshal or equivalent security officer at the unit or activity concerned and at the reserve component provost marshal's office where applicable. The results will be used in planning and assessing physical security programs under AR 190-13.

*c.* The risk analysis may be reviewed and portions of the results changed at the discretion of the installation CONUSA or MUSARC commander or State AG. This could be based on a significant change in risk factors to a specific category of Army property, to a particular unit or activity, or to the overall installation. Any discretionary changes made by the installation commander will be coordinated with the installation provost marshal or equivalent security officer.

## Chapter 3
## Physical Security Standards by Category of Army Property

Section I
Security overview

### 3-1. General

*a.* In this chapter, common types of U.S. Army property are classified in readily understandable categories for quick reference. Guidance for each category of property listed includes references to the primary directives for management and accountability of that category of property and minimum security standards to be implemented.

*b.* Section II of this chapter outlines physical protective, security procedural, and terrorism counteraction measures for particular categories of property maintained at U.S. Army installations or facilities. The measures are categorized according to their risk levels established using the risk analysis procedure in DA Pam 190-51. Risk Level I physical protective and security procedural measures will be treated as minimums. Physical protective and security procedural measures primarily address threats related to theft of the asset. Additional terrorism counteraction measures address terrorist threats related to the killing of people or the destruction of assets. Such measures are only included for asset categories for which they apply.

*c.* Section III of this chapter outlines minimum required security measures to be implemented for other specified categories of property. Although these categories of Army property do not require the conduct of risk analysis using DA Pam 190-51, the principles of risk analysis should be applied and risk factors considered.

*d.* For those categories of U.S. Army property where perimeter fencing is required as a protective measure, the type and quantity of

fencing, including the height (6 or 7 feet) and whether a top guard or other features are required, will be based on the judgment of the installation commander and the guidance found in Field Manual (FM) 19-30. Unless otherwise specified, perimeter fence will meet the requirements of U.S. Army Corps of Engineers Drawing No. 40-16-08, Type FE-S. Copies of this drawing normally may be obtained from the installation engineer. If the drawing is not available locally, requests may be forwarded to the Commander, U.S. Army Corps of Engineers, Huntsville, Division, ATTN: CEHND-ED-ES-l, P.O. Box 1600, Huntsville, Alabama 35807-4301. The minimum height will be 6 feet. Use of North Atlantic Treaty Organization (NATO) standard design fencing is also authorized. Modifications to existing perimeter fences should not be made solely to conform to the requirements of this regulation if the existing fencing provides a similar deterrent to penetration.

*e.* In those instances where security lighting is required, FM 19-30 will be used as a guide in deciding lighting patterns and minimum protective lighting intensities and requirements.

ƒ Conflicts between security and safety requirements must be identified in writing. Waiver or exception requests must list compensatory measures and be forwarded through the local provost marshal and MACOM to HQDA (DAMO-ODL-S) fur approval.

### 3-2. Categories of Army property

Items of property will not always correspond exactly to the categories listed in sections II or III. Some items may fall into two categories. When this situation occurs, the unit commander directly responsible for the asset is responsible for determining the most appropriate category for the item in question. If none is appropriate, the commander will develop and carry out those security procedures and physical protective measures necessary to safeguard the property.

## Section II
## Minimum Security Standards for Categories of Army Property Using Risk Analysis

### 3-3. Aircraft and components at Army aviation facilities

*a. Property management and accountability directives.*

(1) AR 95-1.
(2) AR 190-16.
(3) AR 710-2.
(4) AR 735-5.
(5) DA Pam 710-2-1.

*b. Aircraft with arms, ammunition, and explosives (AA&E) aboard* Army aircraft with AA&E aboard will be secured as indicated in AR 190-11 and this regulation. Army National Guard aircraft with AA&E aboard will be secured as indicated in NGR 190-11 and this regulation.

(1) When not in use, aircraft containing weapons will be parked inside an aircraft parking area. The parking area will be lighted and will have either continuous surveillance or IDS.

(2) When operational readiness permits, weapons mounted on aircraft that are accessible and easily removable will be removed and stored in a secure location. Weapons that remain installed on the aircraft will be made inoperable by removing barrels or firing mechanisms when practicable. Removed components will be stored in a secured location. A secured location is an arms room, an ammunition supply point, an area under continuous armed surveillance, or any structure meeting the requirements for storage of category I or II AA&E in AR 190-11 or NGR 190-11.

*c. Accessible and easily removable components.* Additional security for accessible and easily removable components will be by storage in a secure structure (app B).

*d. Aircraft with classified equipment.* U.S. Army aircraft with classified equipment aboard will be secured as indicated in AR 380-5, Technical Bulletin (TB) 380-41, and paragraph 3-18 of this regulation. Classified components which can be readily removed without damage to them should be placed in secure storage as indicated in AR 380-5.

*e. Physical protective measures.*

(1) *Risk Level I.*

(a) Army aircraft at Army aviation facilities will be secured with manufacturer-installed or approved modification work order ignition and door-locking security devices when not in use. Aircraft undergoing maintenance with duty personnel present and aircraft employed in tactical exercises are exempt.

*(b)* Keys to locking devices and ignitions will be controlled. Key control and accountability must be established per appendix D. Aircraft keys will not be issued for personal retention. Duplicate keys will not serve as operational keys at maintenance facilities.

*(c)* When not in use, aircraft and aircraft components, to include crew member equipment at Army aviation facilities, will be placed in the most secure hangars or structures available. If adequate hangar space is not available, this equipment may be stored on the ramp nearest the facility.

*(d)* When aircraft are not stored in storage structures and when operational requirements permit, keep them in proximity to each other for ease of monitoring and away from the perimeter of the parking area.

(2) *Risk Level II.*

(a) All measures required for Risk Level I will be implemented.

*(b)* Aviation facility aircraft parking areas will be protected by a perimeter fence.

(3) *Risk Level III.*

(a) All measures required for Risk Levels I and II will be implemented.

*(b)* Aviation facility aircraft parking areas will be lighted at night sufficiently to allow security personnel to detect intruders. Airfield lighting will be coordinated with the aviation facility commander for consideration of safety and training issues.

*(c)* IDS should be added to hangars and, where practical, around aircraft parking areas.

ƒ *Security procedural measures.*

(1) *Risk Level I.*

(a) Each Army aviation facility will have a written physical security plan. FM 19—30 will be used as a guide. Aviation facilities located on or close to an Army installation will include the physical security plan as an annex to the installation physical security plan. Aviation facilities located on other than Army property will coordinate the physical security plan with the appropriate host authorities. A copy of the physical security plan will be maintained by the State AG or MUSARC provost marshal for reserve component aviation facilities.

*(b)* Each Army aviation facility will have a physical security officer. Responsibilities of the physical security officer are defined in AR 190-13.

*(c)* For aircraft parked at Active Army aviation facilities and for U.S. Army Reserve (USAR) and Army National Guard (ARNG) activities where guards or roving patrols are available, aircraft will be checked at least every 4 hours by a roving guard.

*(d)* At USAR and ARNG activities where guards or roving patrols are not available, local law enforcement agencies will be requested, in writing, to include the aviation facilities in their patrol areas and to check aircraft parking areas at intervals not exceeding once every 4 hours during nonoperational hours.

*(e)* Access to aviation facility aircraft and aircraft components will be controlled at all times. The airfield will be designated as a restricted area as specified in AR 190-13. Measures such as badges, passes, or similar identification credentials are encouraged.

*(f)* Privately-owned vehicles will be prohibited from the flight line or other areas where aircraft are parked, except when authorized, in writing, by the aviation facility or airfield commander.

(g) Aviation facility auxiliary power units for starting aircraft, vehicle tugs, forklifts, aircraft boarding ladders, and other items that might be used to circumvent existing security measures will be secured during nonduty hours to prevent unauthorized use.

(2) *Risk Level II.*

*(a)* All measures required for Risk Level I will be implemented.

*('b)* Entry to and exit from all buildings associated with the aviation facility, aircraft parking areas, and support equipment storage

areas will be controlled at all times. Entry and exit can be controlled through manpower and procedural means, mechanical means, or electronic means.

*(c)* Aircraft parked at Active Army aviation facilities will be checked at least once every hour by a roving guard.

(3) *Risk Level III.*

(a) All measures required for Risk Levels I and II will be implemented.

*(b)* Guards will provide continuous surveillance of aircraft parked at Active Army aviation facilities. Aviation unit personnel working on or near aircraft may be considered to be equivalent to continuous surveillance.

*(c)* IDS may be installed as an alternative to providing continuous surveillance.

*(d)* At USAR and ARNG facilities where guards or roving patrols are available, aircraft will be checked at least every 2 hours. Where guards or roving patrols are not available, local law enforcement agencies will be requested, in writing, to include USAR and ARNG aviation facilities in their patrol areas, and to check the parking areas at least once every 2 hours during nonoperational hours.

g. *Terrorism counteraction measures.* Due to the likely form of a terrorist attack against these assets, the physical protective measures and security procedural measures established above will also be applicable for protection against terrorist threats. Aviation facilities will develop a terrorism counteraction contingency plan.

### 3-4. Aircraft and components not at Army aviation facilities

The property accountability requirements outlined in the references in paragraph 3-3a will be followed and paragraphs 3-*3b, c,* and *d* will be implemented. Physical protective measures for Risk Level I in paragraph 3-3 will also be implemented. In addition, the security procedures indicated below will apply.

a. Aircraft will be parked, whenever practical, at a Government airfield or civilian airport with an active security program. If a location has no security program and a crew member cannot remain with the aircraft, the aircraft commander will advise aviation facility and local law enforcement authorities of the aircraft location, identification, length of stay, and ways to contact crew members.

*b.* The aircraft will be checked at least once daily by a crew member for tampering, sabotage, and loss or damage.

### 3-5. Vehicles and carriage—mounted/towed weapons systems and components

*a. Property management and accountability directives.*

(1) AR 58-1.

(2) AR 710-2.

(3) AR 735-5.

(4) DA Pam 710-2-1.

(5) DA Pam 738-750.

*b. Army vehicles with weapons or ammunition aboard.* These vehicles will be secured per AR 190-11. When operational readiness permits, weapons mounted on vehicles that are accessible and easily removable will be removed and stored in a secure location. Unless there is an operational necessity determined by battalion or higher level commanders, firing mechanisms on weapons that are not easily removable will be removed from combat vehicle weapon systems and stored in the unit arms room or be under continuous surveillance.

*c. Army vehicles with classified equipment.* These vehicles will be secured per AR 380-5 and paragraph 3-18 of this regulation. Classified components that can be readily removed without damage should be placed in secure storage as indicated in AR 380-5.

*d. Army vehicles when not in use.* These vehicles will be parked in motor poo1s to the maximum extent practicable. The motor pool will be protected by a perimeter fence or dedicated guards. FM 19-30 will be used as a guide for determining fencing requirements.

*e. Physical protective measures.*

(1) *Risk Level I.* Army vehicles parked in noncombat areas will be secured with a locking mechanism. These vehicles will be locked as follows:

(a) *Commercial-design vehicles.* Activate manufacturer installed door and ignition-locking device(s).

*(b) Tactical vehicles and M880 series vehicles.* Immobilize steering wheel with a chain and a U.S. Government approved padlock as specified in TB 9-2300-422-20. Activate installed door and ignition-locking devices. Hood, spare tires, and fuel tank should also be secured with approved locking devices if the local environment warrants this action. Brass padlocks supplied with vehicles may be used to secure vehicles, except those uploaded with AA&E or other sensitive items, and as long as other security measures required by applicable regulations and directives are followed.

*(c) Other Army vehicles.* M1008, 1009, and 1010 series vehicles and commercial utility and cargo vehicles (CUCV) will be secured by activating installed door and ignition locks and immobilizing the steering wheel with chain and U.S. Government approved padlock as specified in TB 43-001-39-7. Alternatively, such vehicles may be stored in a secure structure.

*(d) Material handling equipment.* Material handling equipment (MHE) and other Army vehicles which cannot be secured as indicated in *(a)* through(c) above should have the steering mechanism immobilized or transmission lever locked in the neutral position. Alternatively, these vehicles may be stored in secure structures.

*(e) Signs.* "Off Limits To Unauthorized Personnel" signs will be posted at the activity entrances.

(2) *Exceptions.* Exceptions to this policy are as follows:

*(a)* Vehicles actively employed in tactical exercises and field operations, undergoing test and evaluation, or pending turn-in through property disposal channels.

*(b)* Dispatched emergency, military or security police, courtesy patrol, and interior guard vehicles for brief periods when response time is critical for the successful performance of the operator's or crew's duties. Ignition keys should be removed from unaccompanied vehicles.

*(c)* Trailers, semitrailers, towed weapons systems, and other non-self-propelled vehicles.

*(d)* Inoperable, unserviceable vehicles. Procedures will be implemented to protect these vehicles from cannibalization.

*(e)* Vehicles, without installed locking mechanisms, under the continuous surveillance of a guard or located in a secure storage structure (app B).

*(f)* Vehicles of specific units outside the United States when so designated by the MACOM commander. Basis for a unit exemption will be an impact on readiness. The commander will decide whether locking the unit's vehicles would adversely affect readiness to the extent of jeopardizing the unit's contingency mission.

(g) Fuel tanker vehicles when, in the judgment of the installation commander, locking would create a potential unacceptable hazard to life or property. In this case, compensatory security measures as outlined in paragraph 3-14 will be taken.

(h) Administrative use vehicles, as defined in AR 58-1, when dictated by safety requirements within an ammunition or explosives production or storage area.

(3) *Accessible and easily removable components.* These components, vulnerable to theft because of value or utility, will be removed and secured separately. Additional security for components will be provided by one of the following methods:

*(a)* Storing in a secure storage structure (app B).

*(b)* Storing in a locked, totally enclosed armored vehicle or truck van.

*(c)* Storing in a locked equipment box or similar container secured to an open bed vehicle; for example, in a locked ammunition or tool box chained to the bed of a 2 1/2—ton truck.

*(d)* Securing the item directly to the vehicle by a locally fabricated method.

(4) *Master-keyed locksets.* Use of master-keyed locksets to secure Army vehicles or motor pools will be prohibited except under the following conditions:

*(a)* When the lockset is used within one vehicle to secure the

vehicle and its various storage compartments. Master-keyed locksets will not be used to secure more than one vehicle.

*(b)* When the lockset is used to secure the manifold access doors and hatches of petroleum, oil and lubricants (POL) trucks (one set per truck) and, if they have hardened steel shackles, for the storage compartments of wreckers, heavy equipment, etc. (one set per vehicle). The same set will not be used on more than one vehicle. Master-keyed locks will not be used to secure vehicle steering wheels.

(5) *Keys and locks.* Keys and locks will be controlled according to appendix D.

(6) *Items used to defeat security measures.* Items that can be used to defeat security measures, such as bolt cutters, hacksaws, oxyacetylene torches, axes, or steel rods or bars, will be secured in respective tool kits or other secure locations when not in use.

(7) *Risk Level II.*

*(a)* All measures required for Risk Level I will be implemented.

*(b)* Vehicle parking areas, except those for empty trailers, will be lighted during the hours of darkness.

*(c)* Vehicles will be parked at least 20 feet from the perimeter of the parking area or as far from the perimeter as possible.

(8) *Risk Level III.*

*(a)* All measures required for Risk Levels I and II will be implemented.

*(b)* Ground anchors will be constructed for trailers, semitrailers, and other towed equipment or a cable will be run through all items of such equipment and a lock will be affixed to one end.

*(c)* Vehicles particularly vulnerable to theft, misappropriation, or damage will be placed in secured garages and motor sheds to the maximum extent practicable.

*f Security procedural measures.*

(1) *Risk Level I.*

*(a)* For Active Army installations and for USAR and ARNG units and activities at locations where guards or roving patrols are available, motor poo1s will be checked for tampering, sabotage, loss, and damage not less than once every 4 hours.

*(b)* USAR and ARNG units and activities at locations where guards are not available will request, in writing, that the local law enforcement agency check the security of the motor poo1 at intervals not exceeding 4 hours during nonoperational hours.

*(c)* Privately-owned vehicles will not be permitted in motor pools except that units engaged in deployment exercises may store privately-owned vehicles in the motor poo1 at the discretion of the installation or MUSARC commander, provided security measures are taken to safeguard Army vehicles and components remaining in the motor pool.

(2) *Risk Level IL*

*(a)* Measures required for Risk Level I will be implemented.

*(b)* Entry to and exit from motor poo1s will be controlled. Control of entry and exit may be by guards or locks on gates. Unit personnel working within the motor poo1 may be considered an alternative to guards. Consolidated motor poo1s will have memorandums of understanding to establish joint security procedures.

*(c)* Types of vehicles particularly vulnerable to theft, misappropriation, or damage in the motor poo1 will be segregated. These vehicles will be placed where guards or unit personnel can see them during operating hours and where roving guards can see them during nonoperating hours.

*(d)* On Active Army installations, guards will check the motor pool on an irregular basis, but perform security checks not less than once every 2 hours.

(3) *Risk Level III.*

*(a)* All measures required for Risk Levels I and II will be implemented.

*(b)* The motor pool will be designated a restricted area under AR 190-13.

*(c)* Unit commanders, or their specifically designated representatives, will give written authorization before vehicles are dispatched.

*(d)* Drivers will be checked for possession of a valid dispatch and operator's permit by unit personnel or guards before they depart the motor pool.

*(e)* Continuous surveillance will be made of the motor pool by guards on Active Army installations.

(*/*) IDS may be installed as an alternative to providing continuous surveillance.

(g) At USAR and ARNG activities where guards or roving patrols are available, motor pools will be checked for tampering, sabotage, loss, or damage not less than once every 2 hours. Where guards or roving patrols are not available, local law enforcement agencies will be requested, in writing, to include USAR and ARNG motor poo1s in their patrol areas, and to check the parking areas at least once every 2 hours during nonoperational hours.

*g. Terrorism counteraction measures.* Due to the likely nature of a terrorist attack against these assets, the physical protective measures and security procedural measures established above will also be applicable for protection against terrorist threats.

### 3-6. Communications and electronics equipment and night vision devices

Communications and electronics test, measurement, and diagnostic equipment (TMDE) and other high-value precision equipment, night vision devices that are not part of a weapons system, and tool kits are protected as follows:

*a. Property management and accountability directives.*

(1) AR 710-2.

(2) AR 735-5.

(3) DA Pam 7 10-2-1.

*b. Physical protective measures (Risk Level I).*

(1) Portable items will be provided double barrier protection when not in use, to include training environments and while in transit. Examples of double barrier protection include-

*(a)* A locked or guarded separate building or an enclosed van, trailer, or armored vehicle protected by a perimeter fence.

*(b)* A locked steel cage located in a secure storage structure (app B).

*(c)* A locked, built-in container (bin, drawer, cabinet) or a free-standing locked container located in a secure storage structure (app B).

*(d)* Securely affixing the item to an internal structure of a secure storage structure (apps B and D).

*(e)* Securely affixing the item to a locked vehicle which is under continuous surveillance or in a motor pool (app D).

(2) Nonportable items will be secured in a building with doors and windows locked during the hours the facility is nonoperational. Particularly bulky or heavy items stored outside will be protected by a perimeter barrier.

(3) "Off Limits to Unauthorized Personnel" signs will be posted at the activity entrances.

(4) Equipment will be located in the interior of the facility as far from the exterior as possible.

(5) Tactical communications equipment remaining on vehicles will be secured to the vehicle with a medium security padlock. Vehicles will be secured per paragraph 3-5 of this regulation.

(6) Tool kits will be secured as specified in paragraph 3-22.

*c. Physical protective measures (Risk Level II).*

(1) Measures required for Risk Level I will be implemented.

(2) Portable, pilferage-coded items will be separated from other equipment and stored in a separate, locked, secure room, area, or container with controlled access. Secure rooms will be constructed per secure structure guidance in appendix B of this regulation.

*d. Physical protective measures (Risk Level III).*

(1) All measures required for Risk Levels I and II will be implemented.

(2) The activity will be lighted during the hours of darkness.

(3) Landscaping features greater than 1 foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

(4) IDS will be installed around or on the storage room, area, or container.

*e. Security procedural measures (Risk Level I).*
(1) Access to the equipment storage area will be controlled.
(2) Access to keys, padlocks, and protective seals protecting assets will be controlled per appendix D.
(3) Portable, pilferage-coded items temporarily assigned to a user will be issued on a hand receipt or a locally devised temporary receipt.
*f Security procedural measures (Risk Level ID.*
(1) Measures required for Risk Level I will be implemented.
(2) Privately-owned vehicles will not be permitted to park within 50 feet of the storage facility.
(3) Periodic command-directed inventories will be made as indicated in AR 7 10-2. A copy of the inventory will be kept until the next inventory is conducted.
*g. Security procedural measures (Risk Level III).*
(1) Measures required for Risk Levels I and II will be implemented.
(2) Stock accounting records for portable pilferage-coded items will be reviewed at least monthly by an officer, noncommissioned officer (NCO) (sergeant or above), or civilian employee of equivalent grade. A record of such review will be maintained until completion of the next monthly review.
(3) The activity will be checked at least every 2 hours after normal duty hours by guards on Active Army installations.
(4) Local law enforcement agencies will be requested, in writing, to include USAR and ARNG facilities storing communications and electronics equipment in their patrol areas and to check the facilities at least every 4 hours during nonoperational hours.

### 3-7. Organizational clothing and individual equipment (OCIE) stored at central issue facilities

*a. Property management and accountability directives.*
(1) AR 710-2.
(2) AR 735-5.
(3) DA Pam 710-2-1.
*b. Physical protective measures.*
(1) *Risk Level I.*
*(a)* Stocks will be secured in a separate building or room meeting the security standards in appendix B.
*(b)* "Off Limits To Unauthorized Personnel" signs will be posted at facility entrances.
(2) *Risk Level IL*
*(a)* Measures required for Risk Level I will be implemented.
*(b)* High-value or small, easily pilferable items will be separated from other OCIE and stored in a secure, separate container, room, or building with controlled access.
(3) *Risk Level III.*
*(a)* Measures required for Risk Levels I and II will be implemented.
*(b)* The facility exterior will be lighted during the hours of darkness.
*(c)* IDS will be installed in the facility.
*(d)* Rooms or buildings will be constructed per secure storage structure guidance for at least Risk Level II in appendix B of this regulation.
*(e)* Landscaping features greater than 1 foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.
*c. Security procedural measures.*
(1) *Risk Level I.*
*(a)* Access to the facility and to keys, padlocks, and protective seals protecting assets will be controlled per appendix D.
*(b)* Periodic command-directed inventories will be conducted per AR 710-2.
(2) *Risk Level II.*
*(a)* Measures required for Risk Level I will be implemented.
*(b)* The joint inventory check-out point will be placed next to the facility exit to preclude personnel from remaining in the facility once the OCIE has been inventoried. A copy of the inventory will be retained until the next inventory is conducted.
*(c)* Privately-owned vehicles will not be parked within 50 feet of the storage facility.
*(d)* Trash receptacles will not be located within 50 feet of the facility.
(3) *Risk Level III.*
*(a)* Measures for Risk Levels I and II will be implemented.
*(b)* The facility will be checked at least once every 2 hours by roving guards.

### 3-8. OCIE not stored at central issue facilities

*a.* Risk Level I physical protective measures and the security procedures in paragraph 3—7 will be implemented for OCIE stored centrally in units.
*b.* Issued clothing will be marked as indicated in AR 700-84.
*c.* Individual clothing and equipment of personnel living in troop billets and reserve component personnel will be secured by one of the following means to be determined by the commander:
(1) In a locked wall locker or footlocker.
(2) In a locked duffel bag, further secured to the building structure, or a separate locked room.
(3) Access to reserve component OCIE will be controlled by designated individuals. Locked duffel bags, wall lockers, or footlockers will be placed in a separate locked room or cage. In lieu of a separate room, access to wall lockers may be controlled by modifying the lockers to accept a locking bar or by adding a second hasp and securing the locker with a second lock. Keys to access reserve component OCIE will be placed in the unit key depository and access will be controlled by the unit key custodian.
*d* Consideration should be given to marking items as indicated in appendix C.

### 3-9. Subsistence items stored at commissaries, commissary warehouses, and troop issue subsistence activities (TISAs)

*a. Property management accountability directives.*
(1) AR 30-1.
(2) AR 30-18.
(3) AR 30-19.
(4) AR *735-5.*
*b. Physical protective measures.*
(1) *Risk Level I.*
*(a)* Commissaries, commissary and subsistence warehouses, and TISAs will meet the construction requirements for secure storage structures in appendix B.
*(b)* "Off Limits to Unauthorized Personnel" signs will be posted at entrances to subsistence storage facilities (see AR 420-70).
*(c)* Refrigeration units will be secured with approved locking devices or kept in a room or building meeting the standards for secure storage structures in appendix B.
*(d)* Subsistence items temporarily stored outside the facility, such as in secured vans and reefer trucks, will have protective lighting. Use FM 19—30 as a guide to determine the type of protective lighting.
*(e)* Break areas will be located away from the storage areas.
*(f)* Personal lockers will be in a designated area away from loose or broken containers of subsistence items.
(2) *Risk Level II.*
*(a)* Measures required for Risk Level I will be implemented.
*(b)* Highly pilferable items such as cigarettes, coffee, and health and beauty aids will be placed in a separate locked room, cage, or container under the control of a designated property custodian.
*(c)* Protective seals will be placed on doors and other operable openings into secured vans and reefer trucks in which subsistence items are stored outside the facility.
(3) *Risk Level III.*
*(a)* Measures required for Risk Levels I and II will be implemented.
*(b)* The facility will be lighted during the hours of darkness.
*(c)* IDS will be installed in the facility.

*(d)* Landscaping features greater than 1 foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

*c. Security procedural measures.*

(1) *Risk Level I.*

(a) Access to the facility and to keys and padlocks and protective seals protecting assets will be controlled according to appendix D.

*(b)* Subsistence storage facilities will always be secured when entrances or exits are not under the surveillance of personnel assigned to the facility.

*(c)* Personal packages will be prohibited in ration breakdown and subsistence storage areas.

*(d)* Shipping containers and cases will be inspected to ensure that they are empty prior to being disposed of and cardboard boxes will be flattened before disposal.

(2) *Risk Level II.*

*(a)* Measures required for Risk Level I will be implemented.

*(b)* Personnel entering the storage facility who are not assigned to the activity will be logged in and out or, when practical, escorted. When using the log system, designate the destination of the unassigned person.

*(c)* Accuracy of scales will be tested monthly with known weights or by using a second set of calibrated scales. A written record of the monthly tests will be maintained for a period of 3 months.

*(d)* Highly pilferable items will be spot-checked daily by supervisors to ensure that all items are accounted for. These items will also be inventoried each quarter and a copy of the inventory kept until the next inventory.

*(e)* Trash receptacles will not be located within 50 feet of the facility.

(f) Privately-owned vehicles will not be parked within 50 feet of the storage facility.

(3) *Risk Level III.*

*(a)* Measures required for Risk Levels I and II will be implemented.

*(b)* Highly pilferable items will be inventoried once each month. A copy of the inventory will be kept until the next inventory.

*(c)* The facility will be checked at least every 2 hours after normal operating hours by roving guards.

### 3-10. Subsistence items not at commissaries, commissary warehouses, and troop issue subsistence activities

Risk Level I physical protective measures and the security procedures in paragraph 3-9 will be implemented.

### 3-11. Repair parts at installation level supply support activities and direct support units with an authorized stockage list (ASL)

*a. Property management and accountability directives.*

(1) AR 708-1.

(2) AR 710-2.

(3) AR 735-5.

(4) DA Pam 710-2-1.

*b. Classaied repair parts.* Secured under AR 380 series requirements and paragraph 3-18 of this regulation.

*c. Physical protective measures (Risk Level I).*

(1) Portable repair parts will be secured in the following manner:

*(a)* In a locked, separate building or room, meeting the secure storage structure standards in app B.

*(b)* In a locked, steel cage.

*(c)* In a locked, built-in container (bin, drawer, cabinet) or a free-standing container (desk, wall locker, container express (CONEX)) large and heavy enough to be nonportable with stored parts.

*(d)* To the building in which located or other permanent structure.

(2) Nonportable repair parts will be secured in a building with doors and windows locked during those hours the facility is nonoperational. When bulky or heavy items are stored outside, they will be protected by a perimeter baffler.

(3) "Off Limits to Unauthorized Personnel" signs will be posted at the storage facility entrance (see AR 420-70).

*d. Physical protective measures (Risk Level II).*

(1) Measures required for Risk Level I will be implemented.

(2) Portable, pilferage-coded items will be separated from other stock and stored in a separate room, building, or container with controlled access.

(3) Rooms or buildings will be constructed per secure storage structure standards in appendix B.

*e. Physical protective measures (Risk Level III).*

(1) Measures required for Risk Levels I and II will be implemented.

(2) The storage facility will be lighted during the hours of darkness.

(3) IDS will be installed in the storage facility.

(4) Landscaping features greater than 1 foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

*f. Security procedural measures (Risk Levels I and II).*

(1) Access to storage areas and to keys and padlocks and protective seals protecting these items will be controlled.

(2) Periodic command-directed inventories will be conducted per AR 710-2.

(3) Used parts will be processed as indicated in Department of Defense (DOD) 4160.21-M to recover parts when prescribed and protect and dispose of nonrecoverable pans, and will be protected and disposed of to preclude recycling.

*g. Security procedural measures (Risk Level III).*

(1) Measures required for Risk Levels I and II will be implemented.

(2) The facility will be checked at least every 2 hours after normal operating hours by guards.

(3) Access for pilferage-coded items will be separately controlled.

### 3-12. Repair parts not at installation level support activities and direct support units

*a.* Risk Level I physical protective measures and the security procedures in paragraph 3-11 will be implemented.

*b.* Unit and activity repair parts will be stored in a single area, readily accessible to designated maintenance or supply personnel only.

### 3-13. Petroleum, oils, and lubricants (POL) at bulk storage facilities

*a. Property management and accountability directives.*

(1) AR 703-1.

(2) AR 710-2.

(3) AR 735-5.

(4) DA Pam 710-2-1.

*b. Physical protective measures.*

(1) *Risk Level I.*

*(a)* Construction of storage facilities will be per DOD 4270. 1-M.

*(b)* When not under the surveillance of personnel authorized to dispense the products, POL pumps will be locked and electrical power will be turned off. The electrical power shutoff will be secured. Hoses to pumps will be secured to prevent loss of POL through gravity feed. These measures are not required if pumps are activated by a credit card type device. Use of such devices will be approved by the MACOM concerned.

*(c)* Packaged POL will be stored in structures under secure storage structure standards in appendix B. Large POL packages (for example, 55-gallon drums) will be stored to preclude their use as hiding places for pilfered items.

*(d)* Keys to POL storage areas, equipment, and buildings will be controlled per appendix D.

(2) *Risk Level II.*

chances of return will depend on the ability of the recovering agency to determine the owner through the reporting system. If there is no identifying data on the property, the chances of return are virtually nonexistent.

### C-3. Marking museum weapons and ammunition

Weapons, with or without serial numbers, will be marked with a catalog number as follows:

*a. Location of catalog number.* The numbers should be placed on the inside of the trigger guard or on the breach of the barrel opposite the lock.

*b. Marking methods.*

(1) Semipermanent *markings.* Semipermanent markings can be applied by using a rapidograph or quill pen and non-waterproof black India ink or oil paint (watercolors are not recommended as they may not adhere). After the paint has dried, apply a coat of varnish over the numbers. See paragraph (2) below regarding records maintenance.

(2) *Permanent markings.* Permanent markings can be applied with a scriber or engraving tool. Such labeling, which can never be removed from the object, should be made only by specific arrangement with the responsible curator and written permission of the Center of Military History. This type of labeling is discouraged if the historical value of the item will be impaired through its application; however, if this is the case, a detailed description of the item should be kept. This includes recording potentially unique characteristics such as scratches and discoloration and their dimensions and location. The description will be retained on file by curators. Photographs, especially color, are extremely useful.

### C-4. Marking other Army property

*a. Standard marking system.* Marking property is worthwhile only if it identifies a specific item as belonging to a particular organization. The recommended standard marking of Army property should-

(1) Use a "USA" prefix which alerts the recovering agency that the property belongs to the U.S. Army.

(2) Have a unit identifier. Use the unit identification code. An abbreviation of the office, unit, or activity designation, such as vehicle bumper markings outlined in TB 43-0209, may also be provided.

(3) Include as the last item in the code a sequential number or letter that identifies the specific item from like items in the using organization. This procedure could be used if more than one item of a type exists and no serial numbers exist to distinguish between these items.

*b. Recording marked items.* Records of marked items including a brief description, serial number, and name of individual to whom hand receipted, preferably the user, should be retained on file.

*c. Identifying and locating owning units of Army property.* Usually the installation or unit provost marshal or security officer will be the initiator of action to identify and locate the property owner. The provost marshal or security officer maintains liaison with civilian law enforcement agencies to ensure they are aware of the standard Army marking system and is the point of contact upon recovery of the property. The unit should notify the provost marshal or equivalent security officer when the Army property is determined missing.

## Appendix D
## Keys, Locks, Locking Devices (including Hasps and Chains), and Protective Seals

### D-1. General

*a.* Guidance on procedures for keys, locks, and locking devices (including hasps and chains), and protective seals is contained in this appendix. Additional requirements for AA&E are in AR 190-11.

*b.* Only approved locks and locking devices (including hasps and chains) will be used. All questions regarding the identity of approved commercial equivalent locks and locking devices (including hasps and chains) meeting military specifications shall be addressed to the Naval Civil Engineering Laboratory (NCEL), ATTN: Code L56, Port Hueneme, CA 93043-4328. Personnel can obtain the most current version of these specifications by contacting the NCEL.

*c.* Under no circumstances will any keys, locks, or alternate keys or locks be placed in a security container that contains or stores classified material.

### D-2. Key custodian and alternate custodian

A primary or alternate key custodian is the person who will-

a. Be appointed, in writing, to issue and receive keys and maintain accountability for office, unit, or activity keys.

*b.* Ensure that individuals designated to issue, receive, and account for keys in his or her absence, clearly understand local key control procedures.

*c.* Maintain a key control register at all times to ensure continuous accountability for keys of locks used to secure Government property.

*d.* Be listed on an access roster.

### D-3. Key control register

Keys will be signed out to authorized personnel, as needed, on a key control register. The key control register, DA Form 551 3-R (Key Control Register and Inventory),is approved for use to meet the requirements of this regulation. When not in use, the key control register will be kept in a locked container that does not contain or store classified material and to which access is controlled.

### D-4. Key depository

*a.* A lockable container, such as a safe or filing cabinet, or a key depository made of at least 26-gauge steel, equipped with a tumbler-type locking device and permanently affixed to a wall, will be used to secure keys.

*b.* The key depository will be located in a room where it is kept under 24-hour surveillance or in a room that is locked when unoccupied.

### D-5. Locks

*a.* The use of any master key system or multiple key system is prohibited except as noted elsewhere in this regulation.

*b.* U.S. Government key-operated, pin-locking deadbolts which project at least 1 inch into the door frame or tumbler-type padlocks will be used to safeguard unclassified, nonsensitive Army supplies and equipment if a lock is required. Selection will be based on the value of items protected, mission essentiality, and vulnerability to criminal attack. All questions regarding approved locks and locking devices will be addressed to the NCEL as indicated in paragraph D-l above.

*c.* Padlocks and keys not in use will be secured in a locked container that does not contain or store classified material. Access to the container will be controlled.

### D-6. Key and lock accountability

*a.* Keys and combinations to locks will be accounted for at all times. Keys to locks in use which protect the property of an office, unit, or activity will be checked at the end of each duty day. Differences between keys on hand and the key control register will be reconciled.

*b.* Padlocks and their keys will be inventoried by serial number semiannually. A written record of the inventory will be retained until the next inventory is conducted.

*c.* When a key to a padlock is lost or missing, an inquiry will be conducted and the padlock replaced or recored immediately.

*d.* A key and lock inventory will be maintained which includes a list of all of the following:

(1) *Keys.*

(2) *Locks.*
(3) *Key serial numbers.*
(4) *Lock serial numbers.*
(5) *Location of locks.*
(6) *The number of keys maintained for each lock.* This list will be secured in the key depository.

*e.* Padlocks and keys which do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate.

### D-7. Additional key and lock controls for IDS and key containers

*a.* Keys to IDS (operational or maintenance) or key containers will not be removed from the installation except to provide for protected storage elsewhere. Keys to locks securing key containers will be afforded physical protection equivalent to that provided by the key container itself. Keys to containers and IDS will be maintained separately from other keys, and will be accessible only to those individuals whose official duties require access to them.

(1) A current roster of these individuals will be kept within the unit, agency, or organization.
(2) The roster will be protected from public view.
(3) The roster will be signed by the designated official and will contain the names of those individuals authorized to receive keys from the key custodian (para *d* below).
(4) At no time will keys be in the custody of a person not listed on the roster.

*b.* Keys to containers and IDS may be secured together in the same key container. However, under no circumstances will keys and locks or alternate keys or locks be placed in any security container that contains or stores classified material.

(1) When arms and ammunition are stored in the same areas, keys to those storage areas may be maintained together, but separately from other keys that do not pertain to AA&E storage. The number of keys will be held to the minimum essential. Keys may not be left unattended or unsecured at any time.
(2) Keys required for maintenance and repair of IDS, including keys to the control unit door and monitor cabinet, will be kept separate from other IDS keys. Access will be permitted only to authorized maintenance personnel.
(3) IDS operational keys will be stored in containers of at least 20-gauge steel equipped with GSA-approved low security padlocks or GSA-approved built-in three-position changeable combination locks, or in GSA-approved Class 5 or Class 6 containers that do not contain or store classified material. Combinations will be recorded on SF 700 (Security Container Information), sealed in the envelope provided, and stored in a container per AR 380-5.
(4) Containers weighing less than 500 pounds will be fastened to the structure with bolts or chains equipped with secondary padlocks to preclude easy removal.

*c.* In the event of lost, misplaced, or stolen keys, an investigation will be conducted immediately. The affected locks or cores to locks will be replaced immediately. Replacement or reserve locks, cores, and keys will be secured to preclude access by unauthorized individuals.

*d.* A key and lock custodian will be appointed in writing. Only the commander and the key custodian (or alternate, if appointed) will issue keys to those individuals on the key access roster (para *a* above). Personnel listed on the roster may transfer custody, in writing, among themselves.

(1) The key and lock custodian's duties will also include procurement and receipt of keys and locks and investigation of lost or stolen keys. The key and lock custodian will maintain a record to identify each key and lock and combinations to locks used by the activity, including replacement or reserve keys and locks. The record will show the current location and custody of each key and lock.
(2) A key control register will be maintained at the unit level to-

*(a)* Ensure continuous accountability for keys.
*(b)* Ensure positive control of keys.
*(c)* Establish responsibility for the custody of stored AA&E. DA Form 55 13-R may be used for this purpose. Completed key control registers will be retained in unit files for a minimum of 90 days and then disposed of per established MACOM procedures.

*e.* When individuals are charged with the responsibility for safeguarding or otherwise having keys immediately available, they will sign for a sealed container of keys.

(1) A sealed container is a locked and sealed key container or a sealed envelope (SF 700, per AR 380-5) containing the key or combination to the key container.
(2) When the sealed container of keys is transferred from one individual to another, the unbroken seal is evidence that the keys have not been disturbed. The seal need not be broken for inventory of keys. However, evidence of tampering with a sealed container will require an inventory of the keys and such other action as may be required by the commander concerned.
(3) If the keys are not placed in a sealed container, an inventory of keys will be made by serial number or other identifying information of the key (for example, stamped number on key). The inventory and change of custody will be recorded.
(4) Inventory records will be retained in unit files for a minimum of 1 year and then disposed of per established MACOM procedures.

*f* Combination to locks on vault doors or GSA-approved Class 5 or Class 6 security containers will be changed annually or upon change of custodian, or other person having knowledge of the combination, or when the combination has been subject to possible compromise. Combinations will also be changed when a container is first put into service. The combination shall be recorded using SF 700, sealed in the envelope provided, and stored in a container meeting storage requirements indicated in AR 380-5. No other written record of the combination will be kept. Controls will be established to ensure that the envelopes containing combinations to locks are not made available to unauthorized personnel.

*g.* Replacement of lock cylinders and broken keys for high-security locks may be requested through normal supply channels. Requests will be coordinated through the key control custodian. MACOMs are designated as approval authorities for any deviation in key procurement procedures.

### D-8. Additional lock and key requirements for aircraft and vehicle storage

Facilities in which vehicles or aircraft are stored with sensitive items aboard will be secured by approved secondary padlocks. Aircraft will be secured with manufacturer-installed or approved modification work order door-locking devices when not in use. All hatches and other openings to track vehicles which cannot be secured from the inside will be secured on the outside with approved secondary padlocks.

### D-9. Chains

When a chain is required for security of unclassified, nonsensitive equipment and supplies, specifications for approved chains will be obtained from the NCEL as indicated in paragraph D-l above.

### D-1O. Use and control of protective seals

*a. Purpose of the seal.* The purpose of the seal is to show whether the integrity of a storage facility, vehicle, rail shipment, or container has been compromised. A plain seal is not a lock, although combination items referred to as "seal-locks" are available. The purpose of a seal, no matter how well-constructed, is defeated if strict accountability and disciplined application are not maintained.

*b. Ordering and storing seals.* Seal construction specification should include-

(1) *Durability.* Seals must be strong enough to prevent accidental breakage during normal use.
(2) *Design.* Seals must be sufficiently complex to make unauthorized manufacture of a replacement seal difficult.
(3) *Tamperproof* Seals must readily provide visible evidence of

tampering and be constructed in a way that makes simulated locking difficult once the seal has been broken.

(4) *Individually identifiable.* Seals must have embossed serial numbers and owner identification.

*(5) Ordering and issuing.* A single office on an installation will be responsible for ordering and issuing seals. The source for the seals will be instructed to ship the seals to the attention of a seal custodian in that office.

(6) *Unused seals.* Seals not issued for actual use will always be secured in a locked, metal container with controlled access. Only seal custodians and alternates will have access. Recorded monthly inventories will be conducted to preclude undetected loss of seals.

*c. Accounting for seals.* Seal custodians will maintain seal log-books, preferably in hard cover, rather than in loose-leaf books.

(1) Issue of seals to a using office, unit, or activity custodian will reflect date of issue, name of recipient, and seal serial numbers.

(2) Issue of a seal for actual use by a custodian will reflect the seal number, date and time applied, identification of items to which applied (and location on item if other than main door(s)), and the name of the person applying the seal. For outbound loaded trailers, railcars, and container shipments, the appropriate trailer, railcar, or container number and load destination will be noted.

*d. Application of seals.*

(1) Seal all doors and openings, not merely the main one.

(2) Run seal straps through hasp only once. Seals wrapped around several times become illegible.

(3) Listen for "click" when inserting point of seal into sheath.

(4) To ensure positive closure, tug down on strap and twist the point section inserted into the locking mechanism.

*e. Checking seals.* Commands using seals will develop procedures for checking them. These procedures will include actions to be taken to break a seal and actions to be taken upon finding a broken seal.

*f Disposition of used seals.*

(1) All shipping documents will reflect seal number(s). All seals will be verified with seal log, shipping documents, or other appropriate documents before removal and disposal.

(2) Seals must be defaced sufficiently upon removal so that they cannot be used to simulate a good seal. They may be disposed of in normal trash.

(3) If the user seal log is located on the same installation, the custodian will be advised of the destruction of the seal, or the seal will be returned to the custodian. The custodian will annotate the date and time removed and the name of the individual removing the seal across from the original entry on the seal log.

*g. Changing seals.* The colors of seals will be changed periodically as an additional physical security measure.

# Student Handout 3

This handout contains an extract of selected paragraphs of chapter 5, AR 380-5, Department of the Army Information Security Program, dated 29 September 2000, and graphic facsimiles of Standard Forms 700, 701, and 702 for your information.

**(EXTRACT)**

**Security**

# Department of the Army Information Security Program

**Headquarters**
**Department of the Army**
**Washington, DC**
**29 September 2000**

**UNCLASSIFIED**

## Section II
## Control Measures and Visits

### 6-9. Responsibilities for maintaining classified information.

a. Commands will maintain a system of control measures that ensures that access to classified information is limited only to authorized persons. The control measures will be appropriate to the environment in which the access occurs and the nature and volume of the information. The system will include technical, where appropriate, physical, administrative, personal, and personnel control measures.

*b.* DA personnel granted access to classified information are responsible for protecting classified information of which they have knowledge or that is in their possession or control. DA personnel are personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to classified information. Classified information will be protected at all times, either by storage in an approved security container, or having it under the personal observation and physical control of an authorized individual.

### 6-10. Care during working hours

a. Classified material removed from storage will be kept under constant surveillance and control by authorized personnel. Classified document cover sheets, Standard Forms 703 (TOP SECRET Cover Sheet), 704 (SECRET Cover Sheet), and 705 (CONFIDENTIAL Cover Sheet), will be placed on classified documents or files not in security storage. All items containing classified information, such as drafts, carbons, notes, floppy disks, typewriter and printer ribbons, plates, stencils, worksheets, etc., will be destroyed immediately after they have served their purpose, or protected as required for the level of classified information they contain.

*b.* SF 702 (Security Container Check Sheet) will be displayed conspicuously on each piece of equipment used to store classified material. SF 702 need not be used for facilities secured by high-security locks, provided the key and lock control register provides an audit capability in the event of unsecured facilities. SF 702 is used to record the date and time of each instance when a security container is opened and closed. The following procedures apply:

(1) Properly cleared personnel will record the date and time whenever they unlock or lock the security equipment during the day followed by their initials.

(2) If a security container is locked, and the room in which it is located is to be left unattended, whenever possible, a person, other than the person who locked the safe, will check the container to make sure it is properly secured. The person doing the checking will record the time the container was checked and initial the form. The person who locked the safe will see that the check is made.

(3) Containers not opened during a workday will be checked and the action recorded as in subparagraph (2) above.

(4) Notations will also be made on SF 702 if containers are opened after hours, on weekends, and on holidays, as provided above.

(5) The SF 702 will be retained at least 24 hours following the last entry.

*c.* Reversible “OPEN-CLOSED” or “OPEN-LOCKED” signs will be used on each security container or vault in which classified information is stored. Signs are available through normal supply channels.

*d.* A person discovering a security container or security storage area open and unattended will-

(1) Keep the container or area under guard or surveillance.

(2) Notify’ one of the persons listed on part 1, SF 700 (Security Container Information), affixed to the inside of the security container lock drawer. If one of these individuals cannot be contacted, the duty officer, security manager, or other appropriate official will be notified.

*e.* Individuals contacted when a container or area is found open or unattended will-

(1) Report personally to the location; check the contents of the container or area for visible indications or evidence of tampering, theft, or compromise. If any evidence of tampering, theft, or compromise is noted:

(a) Installation or activity security personnel (if not at the scene) will be immediately notified so that a preliminary investigation can be initiated.

*(b)* The custodian will cease examination of the container and its contents (to prevent destruction of physical evidence) unless otherwise instructed by security personnel.

*(c)* A lock technician will be called to determine the nature of the tampering, and whether the security container is operating properly.

(2) Change the combination and lock the container. If the combination cannot be changed immediately, the security container will be locked and placed under guard until the combination can be changed; or the classified contents will be transferred to another container or secure area.

(3) If not previously accomplished, report the incident to the commander or security manager immediately for action relative to compromise or possible compromise.

## 6-11. End—of—Day security checks

a. Commands that access, process, or store-classified information will establish a system of security checks at the close of each working day to ensure that all classified material is properly secured. Standard Form 701 (Activity Security Checklist), will be used to record these checks. An integral part of the security check system will be the securing of all vaults, secure rooms, and containers used for the storage of classified material; SF 702 will be used to record such actions. In addition, Standard Forms 701 and 702 will be annotated to reflect after-hours, weekend, and holiday activity.

*b.* After-duty-hours security checks of desks may be conducted, provided:

(1) Each military member and civilian employee is notified of local policy and procedures pertaining to after-hours inspections, locking of desks, and maintenance of duplicate keys or combinations. Notification must be in writing, and in advance of any after-hours inspection program.

(2) After-duty-hours inspections are conducted only by military or civilian security personnel, and for the sole purpose of detecting improperly secured classified information.

## 6-12. Emergency planning

Commands will develop plans for the protection, removal, and destruction of classified material in case of fire, flood, earthquake, other natural disasters, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise. The level of detail in the plan and the amount and frequency of testing of the plan is at the command option, subject to MACOM approval, and should be based upon an assessment of the risk which might place the information in jeopardy. In this regard, special concern will be given for locations outside the United States. In preparing emergency plans, consideration must be given to reducing the amount of classified material on hand, including the transfer of information to microforms or removable computer media to reduce bulk, and the storage of less frequently used material at more secure locations. AR 380-40 contains policy for the emergency protection, including emergency destruction under no—notice conditions, of COMSEC material.

## 6-13. Telephone conversations

a. Classified discussions are not permitted in personal residences, in public, in public transportation conveyances (airplane, taxi, etc.), or in any area outside approved spaces on a U.S. Government or cleared contractor facility. Classified information will only be discussed, in telephone conversations, over secure communication equipment, such as a STU-III, and circuits approved for transmission of information at the level of classification being discussed. When discussing classified information, the ability of others in the area, who are not appropriately cleared or do not have a need-to-know, will be taken into consideration to make sure that classified information is not compromised by being heard or otherwise accessed by unauthorized personnel. This includes instances where the installation of STU-III telephones are authorized in personal residences. Non-secure telephones will have DD Form 2056 (Telephone Monitoring Notification Decal) affixed, advising the user that the telephone is subject to monitoring at all times and that use constitutes consent to this. Further guidance on monitoring can be found in AR 380-53.

*b.* As an exception to the policy on classified discussions in certain situations requiring immediate contact and discussion of classified information in off-duty hours, the installation of a secure telephone unit (such as STU-III) can be authorized in personal residences to the extent that MACOM policy permits, up to, and including, the SECRET level. Only the SECARMY is authorized to permit TOP SECRET communications, via approved secure methods, and document storage, in personal residences. The MACOM commander is authorized to permit SECRET communications, via approved secure methods, and document storage in personal residences. This will not be authorized for personal convenience. Where such communications units are permitted, care must be exercised in ensuring that unauthorized personnel, to include family members, are not within hearing distance when classified discussions take place, and that the control key for the communications unit is either personally retained or stored in a discrete location separate from the unit. In such cases, it can be necessary for the custodian of the unit to make notes regarding the classified discussion that occurs over the security telephone. Where this occurs, such classified notes can be retained in the personal residence only until the next duty day. If the next duty day falls during a period of more than one day, leave, Temporary Duty (TDY), or other absence, the material will be delivered for storage to a U.S. Government or cleared contractor facility prior to such absence. While in a personal residence, such classified notes will be safeguarded and under the personal, physical control of the authorized, cleared holder of the notes, at all times.

## 6-14. Speakerphone guidance

a. There has been a lot of questions and debates over the use of speakerphones in Sensitive Compartmented

Information Facilities (SCIF) and other open-storage areas. According to Director of Central Intelligence Directives (DCID)l/21 speakerphones are restricted from common-use areas where sensitive conversations might be picked up inadvertently.

*b.* NSA S412 approves the installation/enablement of speakerphones on National Secure Telephone Systems (NSTS) and Secure Telephone Unit (STU)-III instruments. These systems will only be used in sole-use offices, conference rooms, and similar areas, and all room occupants are required to be aware of the conversations taking place, such as rooms used for contingency planning. The intent of speakerphone approval, rests with the room occupant assuming responsibility for taking the necessary precautions to ensure that the classified discussion is not overheard. STU-IIIs must be configured in such a manner as to prevent speaker enablement in the non-secure mode. Approval for use of non-secure speakerphones on NSTS and STU-III instruments will be granted by NSA S412 on a case-by-case basis.

**(SKIP AHEAD TO PARA 7)**

*c.* Classified discussions are not permitted in personal residences, in public, in public transportation conveyances (airplane, taxi, etc.), or in any area outside approved spaces on a U.S. Government or cleared contractor facility. As an exception to this policy, and in certain situations requiring immediate contact and discussion of classified information in off-duty hours, the installation of a secure telephone unit (such as STU—III) can be authorized in personal residences to the extent that MACOM policy permits, up to, and including, the SECRET level. Only the SECARMY is authorized to permit TOP SECRET communications and document storage in personal residences. This will not be authorized for personal convenience. Where such units are permitted, care must be exercised in ensuring that unauthorized personnel, to include family members, are not within hearing distance when classified discussions take place, and that the control key for the unit is either personally retained or stored in a discrete location separate from the unit. In such cases, it can be necessary for the custodian of the unit to make notes regarding the classified discussion that occurs over the security telephone. Where this occurs, such classified notes can be retained in the personal residence only until the next duty day. If the next duty day falls during a period of more than one day, leave, Temporary Duty (TDY), or other absence, the material will be delivered for storage to a U.S. Government or cleared contractor facility prior to such absence. While in a personal residence, such classified notes will be safeguarded and under the personal, physical control of the authorized, cleared holder of the notes, at all times.

## 7-7. Safeguarding of U.S. Classified Information Located in Foreign Countries

Except for classified information released to a foreign government or international organization, and under the safeguarding of that country or organization, U.S. classified material will be retained in foreign countries only when necessary to satisfy specific U.S. Government requirements. Commanders will take into consideration the additional risk associated with storing, discussing, and processing classified information outside the United States in establishing procedures to implement this regulation. Particular attention will be paid to the foreign release requirements of AR 380-10, making sure that classified material is not accessed by foreign personnel not authorized access to the information, keeping classified holdings to the minimum required, making sure that classified material no longer required is frequently and completely destroyed, making sure that classified discussions and processing are protected from unauthorized access from personnel working in the area, that classified discussions are conducted on secure communications equipment, and requiring that the emergency destruction plan is rehearsed and is practical for execution. U.S. classified material in foreign countries will be stored at:

a. A U.S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

*b.* A U.S. Government activity located in a building used exclusively by U.S. Government tenants, provided the building is under 24—hour control by U.S. Government and U.S. citizen personnel.

*c.* A U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host government control, provided the classified material is stored in security containers approved by the GSA and is placed under 24 hour control by U.S. Government and U.S. citizen personnel.

*d.* A U.S. Government activity located in a building not used exclusively by U.S. Government tenants but which is under host government control, provided the classified material is stored in GSA—approved security containers, which are further secured in a locked room or area, to which only authorized U.S. personnel have access. The room or area will be secured with a 3—position dial combination lock meeting Federal Specification FF-L-2740A (electro-mechanical lock). MACOMs can approve the use of an existing non-FF-L-2740A lock until the lock meeting Federal Specification FF-L-2740A is installed.

## 7-8. Equipment Designations and Combinations

a. There will be no external mark revealing the level of classified information authorized to be stored in a given container or vault. Priorities for emergency evacuation and destruction will not be marked or posted on the exterior of storage containers, vaults, or secure rooms. For identification and/or inventory purposes, each vault or container will bear, externally, an assigned number or symbol not relating to any known security markings. This, along with the SF 702 and the "OPEN—CLOSED" or "OPEN—LOCKED" signs, are the only items permitted on the exterior of the security container. The top of the security container will not be used as a "bookshelf" or paper storage area. Storage of various non—authorized items on the top of storage containers, could lead to classified material being inadvertently left unsecured and/or mixed in with other miscellaneous material.

*b.* Combinations to security containers, vaults, and secure rooms will be changed only by individuals assigned that responsibility in writing (for example, the command security manager) and the appropriate security clearance. Combinations will be changed:

(1) When placed in use.

(2) Whenever an individual knowing the combination no longer requires access.

(3) When the combination has been subject to possible compromise.

(4) At least once annually.

(5) When taken out of service. When taken out of service, built—in combination locks will be reset to the standard combination 50-25—50; combination padlocks will be reset to the standard combination 10-20-30.

(6) Annually, per U.S. Central Registry, when NATO information is stored in the security container, vault, or secure room.

*c.* A record will be maintained for each vault, secure room, or container used for storing classified information, showing location of the container, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. Standard Form 700 (Security Container Information) will be used for this purpose. A current record for all security containers, vault doors, and padlock combinations will be kept on SF 700.

(1) Complete part I and part 2A, SF 700. Include the name and signature of the person making the combination change in item 9, part 1.

(2) Part 1, SF 700 will be posted on the inside of the lock drawer of the security container.

(3) Parts 2 and 2A, SF 700 will be marked with the highest classification of material stored in the container.

(4) Part 2A, SF 700 will be detached and inserted in the envelope. Part 2A, SF 700, used to record a TOP SECRET combination, will be accounted for in the same manner as other TOP SECRET documents, except that a DA Form 969 is not required. Because of the design of the SF 700, the TOP SECRET information would not be disclosed to personnel handling the sealed envelope. Upon change of a TOP SECRET combination, the old Part 2A is automatically declassified, and may be deleted from the TOP SECRET register (or DA Form 3964).

(5) Only part 1, SF 700 need be completed for security containers storing two-person control material. Parts 2 and 2A need be used only if there is a specific need for recording the combination.

*d.* The combination of a container, vault or secure room used for the storage of classified information will be treated as information having a classification equal to the highest classification level of the classified information to be stored inside. Such written records are classified and will be stored in containers approved for the storage of classified information, at the appropriate classification level, at the next higher headquarters. Written records of combinations will not be personally retained in wallets, purses, briefcases, desk drawers, on calendars or note pads, or written "in code" or foreign languages and stored in unapproved locations.

*e.* Access to the combination of a vault or container used for the storage of classified information will be granted only to those individuals who are authorized access to the classified information that is to be stored inside.

*f* Entrances to secure rooms or areas, will be either under visual control at all times during duty hours, to preclude entry by unauthorized personnel, or the entry will be equipped with electric, mechanical, or electro-mechanical access control devices to limit access during duty hours. Section III, of this Chapter, provides standards for these access control devices. Electronically actuated locks (for example, cipher and magnetic strip card locks) and other such locking devices used primarily for duty—hours access control do not afford by themselves the required degree of protection for classified information and must not be used either during or after duty hours as a substitute for the locks prescribed in paragraph 7-4b.

## 7-9. Repair of Damaged Security Containers

Neutralization of lock—outs, or repair of any damage, that affects the integrity of a security container approved for storage of classified information, will be accomplished only by authorized persons who have been the subject of a trustworthiness determination, in accordance with AR 3 80-67, or are continuously escorted while so engaged.

a. With the exception of frames bent through application of extraordinary stress, a GSA—approved security

container manufactured prior to October 1991 (identified by a silver GSA label with black lettering affixed to the exterior of the container) is considered to have been restored to its original state of security integrity as follows:

(1) All damaged or altered parts, for example, the locking drawer, drawer head, or lock, are replaced.

(2) The safe has been drilled immediately adjacent to or through the dial ring to neutralize a lock—out, a replacement lock meeting FF—L—2740A is used, and the drilled hole is repaired with a tapered, hardened tool—steel pin, or a steel dowel, drill bit, or bearing, with a diameter slightly larger than the hole, and of such length that when driven into the hole there will remain at each end of the rod a willow recess not less than 1/8-inch nor more than &frac3/16;—inch deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface.

*b.* In the interests of cost efficiency, the procedures identified in subparagraph a(2) above, should not be used for GSA—approved security containers purchased after October 1991, distinguished by a silver GSA label with red lettering affixed to the outside of the container control drawer, until it is first determined whether warranty protection still applies. To make this determination, it will be necessary to contact the manufacturer and provide the serial number and date of manufacture of the container. If the container is under warranty, a lockout will be neutralized using the procedures described in the Federal Standard FED—STD—809 (Neutralization and Repair of GSA Approved Containers), dated 1 April 1998.

*c.* Unapproved modification or repair of security containers and vault doors is considered a violation of the container or door's integrity and the GSA label will be removed. Thereafter, these safes will not be used to protect classified information except as otherwise authorized in this regulation.

*d.* For technical assistance concerning classified material physical security storage standards, commands can contact the Interagency Advisory Committee on Security Equipment (IACSE). The designated DA representatives to the

U.S. GOVERNMENT PRINTING OFFICE: 1987-170-836

## SECURITY CONTAINER INFORMATION INSTRUCTIONS

1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE.
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

| 1. AREA OR POST (If required) | 2. BUILDING (If required) | 3. ROOM NO. |
|---|---|---|
| 4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE) | | 5. CONTAINER NO. |
| 6. MFG & TYPE CONTAINER | 7. MFG & TYPE LOCK | 8. DATE COMBINATION CHANGED |
| 9. NAME AND SIGNATURE OF PERSON MAKING CHANGE | | |

10. Immediately notify one of the following persons, if this container is found open and unattended.

| EMPLOYEE NAME | HOME ADDRESS | HOME PHONE |
|---|---|---|
| | | |
| | | |



☆ **1. ATTACH TO INSIDE OF CONTAINER**

700-101
NSN 7540-01-214-5372

**STANDARD FORM 700 (8-85)**
Prescribed by GSA / ISOO
32 CFR 2003

**Part 1 (Part 2 is a carbon copy of Part 1) of SF 700, Security Container Information**

**WARNIN** **WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFE-GUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIRE-MENTS.** DETACH HERE

CONTAINER NUMBER

NOT TO SCALE

**COMBINATION**

_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____

**WARNING**

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION

**2A** INSERT IN ENVELOPE **SF 700 (8-85)** Prescribed by GSA / ISOO 32 CFR 2003

**Part 2A of SF 700, Security Container Information**

`

| ACTIVITY SECURITY CHECKLIST | DIVISION/BRANCH/OFFICE | ROOM NUMBER | MONTH AND YEAR |
|---|---|---|---|
| Irregularities discovered will be promptly reported to the designated Security Office for corrective action. | Statement<br>I have conducted a security inspection of this work area and checked all the items listed below. | | |

| TO *(If required)* | FROM *(If required)* | THROUGH *(If required)* |
|---|---|---|

| ITEM | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. Security containers have been locked and checked. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. Desks, wastebaskets and other surfaces and receptacles are free of classified material. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. Windows and doors have been locked (where appropriate) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. Security alarm(s) and equipment have been activated (where appropriate). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| INITIAL FOR DAILY REPORT | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TIME | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



701-101
NSN 7540-01-213-7899

**STANDARD FORM 701 (8-85)**
Prescribed by GSA / ISOO
32 CFR 2003
USAPPC V1.00

## SECURITY CONTAINER CHECK SHEET

**TO** (if required) | **THRU** (if required)

### CERTIFICATION

***I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.***

MONTH/YEAR

| DATE | OPENED BY | | CLOSED BY | | CHECKED BY | | GUARD CHECK (if required) | |
|---|---|---|---|---|---|---|---|---|
| | INITIALS | TIME | INITIALS | TIME | INITIALS | TIME | INITIALS | TIME |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

FOLD HERE – REVERSE FOLD

SECURITY CONTAINER CHECK SHEET

TO (if required) | THRU (if required)

CERTIFICATIO

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE | OPENED BY | CLOSED BY | CHECKED BY | GUARD CHECK (if required)

INITIALS | TIME | INITIALS | TIME | INITIALS | TIME | INITIALS | TIME



702-101
NSN 7540-01-213 7900

**STANDARD FORM 702**
**(8-85)** Prescribed by GSA / ISOO 32 CFR 2003

# Student Handout 4

This Student Handout consists of:

- (SH-4-2) Sample "Arms Room/Unit Key and Lock Inventory" to assist you with unit physical security. It does not provide doctrine, however, you can use this handout to fulfill the requirement to maintain a system to conduct key and lock inventories. (The intent is to provide the first sergeant with a tool to improve key and lock control within the unit.)

- (SH-4-3) Sample key and lock control SOP.

- (SH-4-5) Key Control Register and Inventory, DA Form 5513-R.

| ARMS ROOM/UNIT KEY AND LOCK INVENTORY | PERIOD: JAN 99 to JUN 99 | PAGE 1 OF 2 PAGES |
|---|---|---|
| | PRIMARY KEY/LOCK CUSTODIAN<br>1SG Sam Smith | ALTERNATE KEY/LOCK CUSTODIAN<br>SSG Abernathy |

In accordance with AR190-11, a key (includes IDs) and lock inventory by serial number was conducted on all assigned keys and locks as follows:

| UNIT/ACTIVITY<br>B Co, 3rd Bn, 29th INF | | | | LOCATION<br>Bldg 2540, Ft Bliss, TX 79918 |
|---|---|---|---|---|
| LOCK SERIAL NR. | LOCK LOCATION | NO. OF KEYS ORIGINALLY ISSUED | NO. OF KEYS ON-HAND | REMARKS |
| E66244 | RM 102 | *2* | *0* | *1-SPC MILLS, 1-PVT JONES* |
| E66245 | RM 103 | *3* | *1* | *1-SGT BOYER, 1-CPL PRYOR* |
| E66246 | RM 104 | *7* | *4* | *1-SSG ROSS, 1-SGT TAYLOR, 1-PFC KONRAD,* |
| E66247 | RM 105 | *6* | *4* | *1-SPC MARK, 1-SPC ROLLING* |
| | | | | |
| | | | | |

**NOTE:** *MAINTAIN INFORMATION IN ITALICS, PRINT INFO USING A PENCIL FOR EASY UPDATING, AS REQUIRED.*

## *SAMPLE KEY/LOCK INVENTORY*

**STANDING OPERATING PROCEDURE (SOP)**

# KEY AND LOCK CONTROL

1. PURPOSE. The purpose of this SOP is to provide guidelines for key and lock control procedures for (type in your unit, address, and zip code).

2. KEY CUSTODIAN. The commander will appoint a key custodian to issue and receive keys and maintain accountability for office and classroom keys and locks. The key custodian will designate only authorized individuals to issue and receive keys in his/her absence. The key custodian will ensure that designated personnel are familiar with and clearly understand local key/lock control procedures.

3. KEY CONTROL REGISTER. Only authorized personnel may sign out keys on an as needed basis by using the key control register (DA Form 5513-R, dated August 1993). The key control register will reflect identification of the assigned key number recorded on the key(s), date and hour of issue, printed name and signature of both the person issuing the key(s), and the person receiving the key(s). When the person returns the key(s), the key custodian, or his designated representative, will record the date, time, and sign in the "received by" column on the key control register. When not in use, keep the key control register in a locked container (key box) with controlled access.

4. KEY DEPOSITORY.

a. To secure keys, use a lockable container such as a safe, filing cabinet, or a key box constructed of at least 26 gauge steel and equipped with a tumbler type locking device. Permanently affix key boxes to a wall.

b. Attach a key access roster to the front of the key box. Keep the roster covered with a protective document cover to prevent unauthorized viewing of the roster.

c. Maintain only necessary primary keys in the key box. Store all duplicate keys in a separate locked container.

d. Keep the key box (depository) locked at all times except when issuing, receiving, or conducting key inventories.

e. Locate the key box where it is under constant surveillance or in a room that you lock during non-duty hours.

f. Conduct quarterly inventories of serial numbered keys and make one copy of the inventory. Retain the copy of the inventory in the key box with the key control register.

5. LOCKS.

a. Use only U.S. government, key operated, tumbler type padlocks to safeguard unclassified, nonsensitive Army supplies and equipment. Use the following padlocks based on value of items protected, mission essentiality, and vulnerability to criminal attack.

(1) Padlock, low security, key (without chain), NSN 5340-00-158-3805; (with chain), NSN 5340-00-158-3807.

(2) Padlock, medium security, key, NSN 5340-00-799-8016.

b. Do not use master key (common key) padlock sets.

c. Secure padlocks not in use in a locked container along with their keys. Control access to this container.

6. KEY AND LOCK ACCOUNTABILITY.

a. Check keys and locks used for protecting property in offices or classrooms at the end of each duty day. Reconcile differences between keys on-hand and the key control register. Issue keys for personal retention only if daily turn-in clearly jeopardizes mission readiness or seriously impedes operational effectiveness. Inventory personally retained keys on a "show basis" at least quarterly, and maintain the inventory in the key box.

b. Inventory padlocks and their keys no less than semiannually. Conduct all inventories solely on a "show" basis.

c. Give a serial number to keys which do not have one. Inscribe the serial number on the key as appropriate.

d. When you determine a key to a padlock is missing, remove the padlock from the key control system and replace or record it immediately.

Buford B. Beebee
BUFORD B. BEEBEE
CPT, IN
Commanding

**KEY CONTROL REGISTER AND INVENTORY**

For use of this form see AR 190-11; the proponent agency is ODCSOPS

| **UNIT/ACTIVITY** | **PERIOD COVERED** |
|---|---|
| Co B, USASMA, Fort Bliss, TX 79918 | FROM: 4 Jan 94 TO: |

**KEY CONTROL NUMBER(S)**

**(Insert serial number or other identifying number from the key)**

| | | | |
|---|---|---|---|
| 1. 123456 | 11. | 21. | 31. |
| 2. 234567 | 12, | 22, | 32, |
| 3. 345678 | 13. | 23. | 33. |
| 4. 456789 | 14. | 24. | 34. |
| 5. 567890 | 15. | 25. | 35. |
| 6. 678901 | 16. | 26. | 36. |
| 7. 789012 | 17. | 27. | 37. |
| 8. 901234 | 18. | 28. | 38. |
| 9. 012345 | 19. | 29. | 39. |
| 10. | 20. | 30. | 40. |

KEY ISSUE AND TURN IN

| KEY NUMBER | ISSUED (Date/Time) | ISSUED BY (Printed Name/Signature) | ISSUED TO (Printed Name/Signature) | TURNED IN (Date/Time) | RECEIVED BY (Printed Name/Signature) |
|---|---|---|---|---|---|
| 2 | 4 Jan 00 0800 | JAMES OLSEN | JOE STRANGE | 4 Jan 00 1610 | JAMES OLSEN |
| | | **JAMES OLSEN** | *JOE STRANGE* | | **JAMES OLSEN** |
| 4 | 5 Jan 00 1000 | JAMES OLSEN | ABEL WILLY | 5 Jan 00 1630 | ABEL WILLY |
| | | **JAMES OLSEN** | *ABEL WILLY* | | *ABEL WILLY* |
| 6 | **10 Jan 00** 0800 | JAMES OLSEN | BENJAMIN GAY | **10 Jan 00** 1000 | BENJAMIN GAY |
| | | **JAMES OLSEN** | *BENJAMIN CROOKS* | | *BENJAMIN CROOKS* |
| 9 | **2 Feb 00** 1000 | JAMES OLSEN | JOHN CROOKS | | |
| | | **JAMES OLSEN** | *JOHN CROOKS* | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

DA Form 5513-R, AUG 93 DA FORM5513-R, MAR 86, IS OBSOLETE *(Graphic Facsimile)* **USAPPC V2.00**

**KEY ISSUE AND TURN IN** (*Continued*)

| KEY NUMBER | ISSUED (Date/Time) | ISSUED BY (Printed Name/Signature) | ISSUED TO (Printed Name/Signature) | TURNED IN (Date/Time) | RECEIVED BY (Printed Name/Signature) |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**INVENTORIES (JOINT/SEMIANNUAL)**

| DATE | PRINTED NAME/SIGNATURE | DATE | PRINTED NAME/SIGNATURE |
|---|---|---|---|
| 4 Jan 00 | JAMES OLSEN<br>JAMES OLSEN | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

PAGE 2, DA FORM 5513-R, AUG 93 (***Graphic facsimile***) *USAPPC V2.00*